Rozdział 4

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Bankowość internetowa

1. Pojęcie i charakterystyka bankowości internetowej

Następnym, z wymienionych rodzajów bankowości elektronicznej, jest bankowość internetowa. Odkąd Internet stał się ogólnodostępnym na całym świecie środkiem łączności, także banki zainteresowały się tym medium, widząc w nim spory potencjał w dostępie do klienta indywidualnego banku. Powstanie bankowości internetowej, która stała się alternatywą dla bankowości oddziałowej i jej szybki rozwój spowodowały że Internet zaczął być kanałem dystrybucji usług bankowych. Od tej chwili klient banku, bez wychodzenia z domu, mógł dokonywać sprawdzenia stanu swojego konta, mógł założyć lokatę, uzyskać pożyczkę gotówkową, a także dokonać przelewu. Można śmiało zaryzykować stwierdzenie, iż jesteśmy skazani na posiadanie konta internetowego w banku. Potwierdza to fakt, że coraz więcej osób korzysta z tej możliwości, w zabieganej rzeczywistości coraz bardziej cenimy swój czas, a dostęp do konta internetowego umożliwia dokonywanie przelewów niezależnie od miejsca, w którym się znajduje klient banku.

Bankowość internetowa, zdaniem A.J. Grandysa, jest kombinacją technologicznych i organizacyjnych innowacji, rozszerzającą tradycyjne formy usług finansowych oraz kreującą całkowicie nowe usługi świata cyberprzestrzeni[254], przez co umożliwia klientowi kontakt z bankiem poprzez sieć internetową, za pośrednictwem zwykłej przeglądarki internetowej (np. Internet Explorer, Mozilla Firefox), również w urządzeniach mobilnych typu smartfon lub tablet. Nie jest wymagane, aby użytkownik instalował jakiekolwiek dodatkowe oprogramowanie, wystarczy stały dostęp do Internetu lub dostęp na czas wykonywania operacji bankowych.

Bankowość internetową można zdefiniować, jako formę świadczenia usług bankowych za pośrednictwem sieci internetowej, z wykorzystaniem standardowego oprogramowania (przeglądarka internetowa) lub oprogramowania dotykowego do komunikacji z bankiem[255].

[254] Grandys A. J. 1999: Usługi finansowe w rzeczywistości wirtualnej – kartowe doświadczenia, „Bank" nr 9, s. 40.

[255] Szwajkowska G. i in.: op. cit., s. 24.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Pierwszym bankiem świadczącym usługi za pośrednictwem Internetu był amerykański Security First Network Bank, który powstał w 1995 roku w Stanach Zjednoczonych[256]. Natomiast w Polsce usługi bankowe świadczone przez Internet, w październiku 1998 roku, jako pierwszy wprowadził Powszechny Bank Gospodarczy, który w wyniku fuzji tworzy obecnie Bank Pekao SA, poprzez stworzenie Oddziału Elektronicznego, który w wyniku połączenia z Centrum Bankowych Usług Telefonicznych od listopada 1999 roku funkcjonuje jako Centrum Bankowości Elektronicznej TELEPEKAO 24. W ślad za nim poszły również inne banki. W roku 2003 znaczna część oddziałów bankowych oferowała usługi poprzez Internet, z których korzystało 1,3 mln klientów, w tym niewiele ponad 120 tys. stanowią przedsiębiorstwa[257].

Rozwój serwisów bankowości internetowej przebiegał w następujących etapach:

1) informacyjny – obejmujący prezentację oferty usług banku, informacje o banku,
2) interaktywny (pasywny) – umożliwiający przeglądanie sald na rachunkach i kontakt z bankiem,
3) transakcyjny – pozwalający na wykonywanie w sposób zdalny standardowych operacji finansowych,
4) strategiczny – umożliwia interaktywne zarządzanie finansami osobistymi i firmowymi, w tym szeroki dostęp do oferty produktów bakowych, ubezpieczeniowych, usług maklerskich i doradztwo[258].

Charakterystycznymi cechami bankowości internetowej są między innymi: brak konieczności bezpośredniego kontaktu klienta z bankiem i wynikająca z tego oszczędność czasu; wysoka funkcjonalność serwisów bankowych, w tym dostępność wszystkich standardowych usług, które świadczone są w oddziałach banku; całodobowy dostęp do usług bankowych; zadowalający poziom bezpieczeństwa transakcji i środków zgromadzonych na rachunku, przy założeniu przestrzegania przez klienta podstawowych zasad bezpieczeństwa; możliwość jednoczesnej i automatycznej obsługi wielkiej liczby klientów w czasie rzeczywistym; ograniczenie do minimum obiegu papierowych dokumentów; brak ograniczeń terytorialnych; niższe koszty realizacji transakcji w porównaniu z obsługa klientów w oddziałach banku oraz niższe koszty obsługi dla banku[259].

[256] Ryznar Z. 1997: Elektroniczna bankowość, „Bank" nr 10.
[257] Fitta G. 2003: Rewolucja trwa, „Gazeta Bankowa" nr 12, s. 22.
[258] Szwajkowska G. i in.: op. cit., s. 24.
[259] Ibidem, s. 24-25.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

W praktyce zetkniemy się z różnorodną klasyfikacją bankowości internetowej. Świecka wprowadza podział banków świadczących swoje usługi za pośrednictwem Internetu, ze względu na:

1. Charakter działalności:
   a) MODEL I – banki internetowe działające w sieci i posiadające swoje oddziały stacjonarne, które wykorzystują Internet jako alternatywny kanał dystrybucji usług bankowych. Są to zatem banki, w których klient podczas zakładania konta posiada do niego dostęp zarówno poprzez placówkę bankową, a także poprzez Internet i inne media elektroniczne. W chwili obecnej ten model jest najpopularniejszy w grupie banków świadczących usługi poprzez Internet;
   b) MODEL II – banki, które działają wyłącznie w sieci, czyli tzw. banki wirtualne, które wykorzystują Internet jako główny kanał dystrybucji usług bankowych. Banki te nie posiadają tradycyjnych oddziałów bankowych (przykładem może być mBank);
   c) MODEL III – banki internetowe powstałe w ramach banków stacjonarnych, które funkcjonują jako oddzielne elektroniczne oddziały tychże banków niemające połączenia z kontem w oddziale tradycyjnym (przykładem mogą tu być Telepekao w Pekao SA, e-pko w PKO BP SA).
2. Formę działalności:
   a) pasywna – polega ona na przeglądaniu informacji, np. sprawdzanie stanu konta, wgląd w historię rachunku bez możliwości ingerencji. Forma ta należy już do rzadkości;
   b) półaktywna – umożliwia dostęp do uprzednio zdefiniowanych operacji;
   c) aktywna – polega na aktywnym działaniu w ramach prowadzonego rachunku bankowego, np. zlecanie przelewów, założenie lokaty, itp.[260]

Banki, które świadczą swoje usługi za pośrednictwem Internetu również różnią się zakresem, różnorodnością i rozmaitością świadczonych usług. W chwili obecnej możemy wyróżnić trzy zasadnicze poziomy ofert bankowych stosowanych przez banki:

[260] Świecka B.: op. cit., s. 34.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

1. Oferta podstawowa – oferowana przez większość banków. Bank oferuje swoim klientom najprostsze usługi – takie, które nie wymagają połączenia systemu bankowości internetowej z zewnętrznymi systemami informatycznymi. Zwykle klient może sprawdzić saldo rachunku, obejrzeć historię transakcji, założyć lub rozwiązać lokatę terminową, przesuwać środki między kontami na rachunku. Dodatkowe funkcje oferowane przez wiele banków od samego początku to np. umieszczone na stronie internetowej aktywne kalkulatory liczące oprocentowanie lokat i tym podobne.
2. Oferta rozszerzona – wzbogaca ofertę podstawową przede wszystkim o możliwość dokonywania płatności na zewnątrz. Odbywa się to przez wypełnienie odpowiedniego formularza na stronie internetowej. Klient może też zwykle obejrzeć stan swojego zlecenia, a jeśli nie zostało jeszcze zrealizowane – nawet je odwołać.
3. Oferta zaawansowana – zawiera opisane wyżej usługi wchodzące w skład oferty podstawowej i rozszerzonej. Oferta zaawansowana obejmuje natomiast usługi wychodzące poza to, co można znaleźć w tradycyjnych oddziałach – wykorzystujące potencjał Internetu, jego interaktywność, multimedialność i elastyczność. Generalnie, celem banku wprowadzającego ofertę zaawansowaną jest zdobycie przewagi konkurencyjnej poprzez strategię dyferencjacji; sama oferta rozszerzona jest łatwa do skopiowania i nie zapewnia trwałej przewagi. W konsekwencji, bank dąży do możliwie trwałego związania ze sobą klienta przez oferowanie mu czegoś więcej niż tylko same usługi bankowe. Aby to osiągnąć, banki wzbogacają swoje serwisy internetowe na wiele sposobów, np. aktualna informacja, notowania giełdowe, usługi maklerskie, fundusze inwestycyjne, możliwość zakupu produktów innych firm, itp.[261].

Podkreślenia wymaga fakt, iż kanał internetowy w przypadku bankowości elektronicznej może funkcjonować jako uzupełnienie lub ekwiwalent standardowej formy świadczenia usług bankowych (obok placówek bankowych), lub jako jedyny kanał dystrybucji usług bankowych (bank internetowy, wirtualny)[262].

Założenie konta bankowego umożliwiającego korzystanie z usług bankowości internetowej jest niezmiernie proste. Wystarczy do banku złożyć

[261] Grzechnik J. 2000: Bankowość internetowa, Internetowe Centrum Promocji, Gdańsk, s. 37-41.
[262] Szwajkowska G. i in.: op. cit., s. 25.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

wniosek o udostępnienie systemu bankowości internetowej. Wniosek taki można przesłać drogą elektroniczną, wypełniając stosowny formularz na stronie internetowej banku. Następnie, w placówce banku, podpisuje się umowę ramową o korzystanie z systemu bankowości internetowej. Oczywiście w pierwszej kolejności należy posiadać komputer z dostępem do Internetu.

Z posiadaniem internetowego konta bankowego związanych jest szereg zalet, o czym informują banki na swoich stronach internetowych i w reklamach, w tym w szczególności:

- niczym nieograniczony i bezpłatny dostęp do rachunku bankowego (24 godziny na dobę, siedem dni w tygodniu, z każdego miejsca na świecie),
- możliwość sprawdzenia salda i historii dokonanych transakcji na koncie w każdej chwili,
- możliwość doładowania konta telefonu komórkowego,
- składanie i modyfikacja zleceń stałych,
- sprawdzanie salda karty kredytowej i spłacanie zadłużenia tej karty,
- możliwość wydruku potwierdzeń dokonanych transakcji,
- możliwość zarządzania funduszami inwestycyjnymi.

W świetle powyższego stwierdzić można, że bankowość internetowa, to w chwili obecnej jedna z najdynamiczniej rozwijających się gałęzi bankowości. Według raportu netB@nk, udostępnionego przez ZBP na koniec IV kwartału 2014 roku, liczba klientów indywidualnych posiadających dostęp do bankowości internetowej wynosiła 25 120 718 osób. W IV kwartale 2014 roku nastąpił wzrost osób posiadających dostęp do bankowości internetowej o 2,99% (w stosunku do III kwartału 2013 roku wzrost ten wynosił 14,91%). Wzrosła również o 3,53% liczba aktywnych użytkowników bankowości internetowej i na koniec IV kwartału 2014 roku wynosiła ona 13 060 508 osób[263]. Zdaniem ZBP może być to sygnałem, że klienci indywidualni racjonalizują swoją aktywność i rezygnują z rachunków, z których do tej pory nie korzystali.

[263] Źródło: raport netB@ank http://zbp.pl/ (dostęp 25.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

2. Przestępstwa w bankowości internetowej

Dokonywanie transakcji za pośrednictwem sieci Internet, jak podkreślają Kaszubski i Obzejta, związane jest nierozerwanie z koniecznością wykorzystywania do tego celu urządzeń elektronicznych i łączy telekomunikacyjnych. Transakcje te odbywają się w środowisku wirtualnym, które charakteryzuje się tym, iż zapewnia stronom dokonującym transakcji wysoki stopień anonimowości, a konsekwencją tego stanu rzeczy jest duży margines możliwości pozyskania przesyłanych podczas transakcji danych przez osoby trzecie[264]. Stąd też bankowość internetowa nie jest wolna od zagrożeń przestępczością.

W przedmiotowym rozdziale omówione zostaną poszczególne przestępstwa w bankowości internetowej.

2.1. Włamanie do komputerowych systemów informatycznych i telekomunikacyjnych

Poza przestępstwami związanymi z wykorzystaniem kart płatniczych, sprawcy popełniają szereg innych przestępstw powiązanych z bankowością elektroniczną. Jednym z nich jest włamanie się do komputerowych systemów informatycznych i telekomunikacyjnych w celu uzyskania danych dotyczących numerów kart płatniczych i numerów kodów PIN oraz kierowanych do bankomatów potwierdzeniach autoryzacyjnych.

W tym wypadku działania sprawcy wyczerpują znamiona wskazane w art. 267 § 1 k.k. – tzw. naruszenie tajemnicy informacji („Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie") zagrożonego karą grzywny, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Obecne brzmienie przedmiotowego artykułu wprowadzone zostało nowelizacją kodeksu karnego z dnia 24 października 2008 roku[265], która była

[264] Kaszubski R., Obzejta Ł.: op. cit., s. 401.

[265] Ustawa z dnia 24 października 2008 r. o zmianie ustawy kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

wynikiem implementacji polskiego prawa karnego do decyzji ramowej Rady Unii Europejskiej 2005/222/WSiSW z dnia 24 lutego 2005 roku w sprawie ataków na systemy informatyczne[266]. Wspomniana decyzja zobowiązywała państwa członkowskie Unii Europejskiej do podjęcia niezbędnych środków mających na celu kryminalizację następujących zachowań:

1. Nielegalny dostęp do systemów informatycznych.
2. Nielegalna ingerencja w system.
3. Nielegalna ingerencja w dane.
4. Kierowanie, pomaganie i podżeganie oraz usiłowanie, w zakresie określonych wyżej czynów.

Zatem, w myśl przepisów art. 267 § 1 k.k., poza wypadkami, które wynikają z upoważnienia ustawowego (m.in. w art. 218 § 1 k.p.k., art. 237 § 1 i 2 k.p.k., czynności operacyjno-rozpoznawcze[267] prowadzone w oparciu o stosowne przepisy prawne), karalne są następujące przejawy naruszenia tajemnicy informacji (korespondencji):

1) otwieranie bez upoważnienia zamkniętego pisma,
2) podłączanie się do sieci telekomunikacyjnej (podsłuch telefoniczny),
3) przełamywanie albo omijaniu elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia informacji (tzw. *hacking*).

Czynność sprawcza przestępstwa z art. 267 § 1 k.k. polega na uzyskaniu przez sprawcę dostępu do informacji, która nie była dla niego przeznaczona, w wyniku podjęcia czynności wymienionych w cytowanym przepisie. Warto podkreślić, iż znowelizowane brzmienie omawianego przepisu, gdzie zwrot „uzyskuje dostęp", zastąpił zwrot „uzyskuje informację", pozwala na przypisanie odpowiedzialności karnej nie tylko w sytuacji, gdy sprawca zapoznał się z treścią informacji, ale także wtedy, gdy przejmuje władztwo nad nośnikiem informacji, kopiuje zapis informacji, czy omija, przełamuje zabezpieczenia, uzyskując w ten sposób dostęp do informacji[268]. Przed nowelizacją brzmienia omawianego artykułu dla bytu przestępstwa nie było

[266] Dz. Urz. UE L 69/67 z 16.03.2005 r.

[267] Czynności operacyjno-rozpoznawcze to z reguły „niejawne działania organów ścigania, realizowane w celach informacyjnych, prewencyjnych, wykrywczych lub dowodowych (a w przypadku służb wywiadowczych mających ponadto znaczenie polityczne, militarne lub gospodarcze)" – Konieczny J. 2008: Czynności operacyjno-rozpoznawcze, „Kryminalistyka" (red. Widacki J.), Warszawa, s. 125.

[268] Hałas R.: Komentarz do art. 267 KK [w:] Grześkowiak A., Wiak K.: op. cit., s. 1144.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

wystarczające, aby sprawca np. pismo otworzył, ale aby je również przeczytał, zapoznając się w ten sposób z jego treścią.

Czynności opisane w art. 267 § 1 k.k. polegają również na uzyskaniu dostępu do informacji poprzez podłączenie się do sieci teleinformacyjnej, przez co należy rozumieć przyłączenie do takiej sieci urządzenia, którego zadaniem jest umożliwienie pozyskania przekazywanych za jej pośrednictwem informacji[269]. Siecią teleinformatyczną, zgodnie z definicją zamieszczoną w art. 2 pkt 35, ustawy z dnia 16 lipca 2004 roku o prawie telekomunikacyjnym[270], są: „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju".

Czynności opisane w art. 267 § 1 k.k. mogą polegać również na przełamaniu albo omijaniu zabezpieczenia elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia. Przez takie działanie rozumieć będziemy uzyskanie dostępu do treści informacji chronionych hasłem, kodem dostępu, zabezpieczeniem wykorzystującym odciski linii papilarnych itp.[271]

W jednym z wyroków Sąd Apelacyjny w Szczecinie[272] stwierdził, że nie stanowi przestępstwa z art. 267 § 1 k.k. bezprawne posługiwanie się hasłami lub kodami umożliwiającymi dostęp do informacji. Nie do zaaprobowania, zdaniem sądu, pozostaje przy tym także stanowisko aby nielegalne, tj. bez zgody posiadacza, czy też nawet przy użyciu podstępu, uzyskanie kodów i haseł dostępu do konta bankowego tożsame było pojęciu przełamania.

Może się również zdarzyć, że użytkownik uzyska nieautoryzowany dostęp do bezprzewodowej sieci komputerowej wi-fi. Oznacza to faktycznie, iż osoba, która np. w sposób przypadkowy podłączy się do sieci wi-fi, uzyska nie tylko dostęp do wszystkich komputerów oraz urządzeń pracujących w tej sieci, co jest w efekcie tożsame ze *sniffingiem*, a więc podsłuchiwaniem całego ruchu w tej sieci, ale także uzyska dostęp do informacji znajdujących się w tych komputerach. Łatwo można sobie także wyobrazić zupełnie przypadkowe podłączenie się do niezabezpieczonej sieci bezprzewodowej wi-fi innego użytkownika – np. sąsiada z bloku mieszkalnego, co w efekcie

[269] Ibidem.
[270] Dz. U. z 2014 r., poz. 243.
[271] Hałas R.: op. cit., s. 1144.
[272] Wyrok z dnia 14.10.2008 r., sygn. akt II AKa 120/08.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

prowadzi do uzyskania nieuprawnionego dostępu do cudzego systemu komputerowego, przy czym jeżeli taki użytkownik przewidywał taką możliwość i z nią się godził, poniesie on każdorazowo odpowiedzialność karną z art. 267 § 2 k.k.[273] („Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego").

2.2. Przestępstwo *phishingu*

2.2.1. Wyjaśnienie pojęcia phishing i jego geneza

Bankowość internetowa stanowi obecnie jedną z tych usług bankowych, która obarczona jest najwyższym potencjalnym zagrożeniem i ryzykiem. Ryzyko to wynika w głównej mierze z zagrożenia atakami przeprowadzanymi w Internecie. Coraz częściej na stronach internetowych banki ostrzegają swoich klientów przed zagrożeniem, jakie w chwili obecnej stanowi tzw. *phishing*. *Phishing* jest jeszcze jedną metodą, która z powodzeniem wykorzystywana jest przez internetowych oszustów.

Termin „phishing" powstał w połowie lat 90. XX w. w środowisku krakerów, którzy próbowali wykraść hasła do kont w serwisie AOL[274]. Podszywając się pod pracowników tej firmy, wysyłali wiadomości e-mail z prośbą o podanie hasła w celu rzekomej weryfikacji konta. Niekiedy *phishing* tłumaczy się jako *password harvesting fihsing* (ang. łowienie haseł), choć niektórzy twierdzą, że pochodzi od nazwiska Briana Phisha, który podobno jako pierwszy, jeszcze w latach 80. XX w., stosował socjotechnikę do wykradania numerów kart kredytowych[275]. Tak też można ująć główną ideę działania sprawców tego przestępstwa, która w skrócie sprowadza się do nakłonienia klienta do ujawnienia tajnych informacji osobowych, haseł oraz danych finansowych. Zjawisko *phishingu* po raz pierwszy opisano już w roku 1987. Sama nazwa „phishing" pojawiła się jednak dużo później, w 1996 roku, w hakerskim magazynie „2600"[276].

[273] Koszut R. 2008: Cyberpornografia i hacking – wybrane aspekty proponowanej nowelizacji prawa karnego, „Boston IT Security Review" nr 5, s. 36.

[274] AOL (od America OnLine) – jeden z głównych dostawców usług internetowych powstały w 1983 roku jako Quantum Computer Services, później posługujący się nazwą America Online. http://pl.wikipedia.org/wiki/AOL (dostęp 10.03.2015).

[275] Janus R., Delio M. 2005: Niebezpieczne wędkowanie, „PC World Komputer" nr 04, wydanie internetowe: http://www.pcworld.pl/artykuly/47038/Niebezpieczne.wedkowanie.html (dostęp 10.03.2015).

[276] Gajewski M., Phishing – łowienie naiwnych, „CHIP" 11/2009, wydanie internetowe: http://www.chip.pl/artykuly/trendy/2009/11/phishing-lowienie-naiwnych?b_start:int=0 (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Podkreślić należy, że choć *phishing* wyodrębniany jest jako osobna kategoria przestępstw internetowych, to często jest utożsamiany z innymi przestępstwami internetowymi, jak chociażby *spoofing*, o którym będzie mowa w dalszej części rozdziału. Bierze się to z faktu, iż udawanie banku przez włamywaczy jest najczęściej wykorzystywanym sposobem uzyskania od beneficjentów poufnych danych. *Phishing* nie ogranicza się wyłącznie do tej metody. Wykorzystywane są również inne rozwiązania pozwalające pozyskać poufne informacji od klientów. Przykładem mogą tu być tzw. *keyloggery,* aplikacje, które umożliwiają sprawdzenie, jakie klawisze z klawiatury komputera były naciskane przez klienta podczas logowania, czy umieszczanie w plikach graficznych niebezpiecznych kodów itp. Generalnie *phishing* bazuje, podobnie jak *spoofing*, na narzędziach socjotechniki oraz lukach w oprogramowaniu wykorzystywanym przez klienta[277].

Nieodłącznie z pojęciem *phishingu* wiąże się pojęcie *phisher,* określające osobę trudniącą się *phishingiem*. *Phisher* wykorzystuje wiadomości pocztowe wysyłane podobnie jak spam, w dużych ilościach, próbując w ten sposób nakłonić swoje potencjalne ofiary do odwiedzenie spreparowanej przez niego strony internetowej, która do złudzenia przypomina prawdziwą witrynę np. stronę internetową banku. Podszywa się pod godnego zaufania pracownika banku czy administratora portalu i ostrzega przed zablokowaniem konta, jeśli potencjalna ofiara nie odwiedzi firmowej strony (oczywiście podrobionej) i nie wprowadzi, rzekomo w celu potwierdzenia, swoich osobistych danych. Większość osób nie daje się oszukać na tego typu przedsięwzięcia, jednak z danych przedstawionych przez Anti-Phishing Working Group wynika, że prawie 5 procent osób odpowiada na apel *phishera* – a to znacznie więcej niż niecały procent odpowiadających na zwykły spam[278].

Początkowo *phisherzy* udawali pracowników AOL i wysyłali do użytkowników komputerów osobistych poprzez komunikator internetowy wiadomość, prosząc ich o podanie hasła do konta. Argumentowali to potrzebą weryfikacji konta lub potwierdzenia danych na rachunku. Będąc już w posiadaniu tych informacji, włamywacze spisywali dane kart kredytowych i wykorzystywali je następnie do własnych celów. Zjawisko to szybko stało się plagą, co spowodowało, że nowe wersje komunikatora AOL witały użytkowników komunikatem „żaden z pracowników AOL nigdy cię nie zapyta o twoje hasło lub dane do opłacenia rachunku". Niestety, to nie pomogło – użytkownicy komunikatora AOL nadal wierzyli wiadomościom od anonimów na

[277] Źródło: http://bankowoscinternetowa.republika.pl/html/Bezp.html (dostęp 10.03.2015).
[278] Janus R., Delio M.: op. cit.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

komunikatorach. AOL skutecznie z tym zjawiskiem poradził sobie dopiero pod koniec 1997 roku. *Phisherzy* wiedzieli już jednak, że skoro sztuczka zadziała w jednej sieci, to zadziała w całym Internecie[279]. I mieli rację.

Dalszym sporym atakiem *pisherów* było wyłudzenie danych osobowych od klientów instytucji E-gold w czerwcu 2001 roku. Włamywacze, tuż po atakach na World Trade Center w Nowym Jorku w 2001 roku, zgłosili się do klientów, żądając niezwłocznego potwierdzenia swoich danych personalnych w związku z „możliwą wojną na terenie Stanów Zjednoczonych i potrzebą ochrony ekonomii kraju". Jak łatwo możemy się domyślić, przerażeni Amerykanie i tym razem dali się nabrać. Trzy lata później *phishing* uznany został przez większość instytucji zajmujących się zwalczaniem cyberprzestępczości za plagę i jedno z największych zagrożeń w Internecie. Powszechność *phishingu* jest olbrzymia. Przypuszcza się, że obecnie w Internecie krąży więcej fałszywej korespondencji niż autentycznej[280].

Metoda przestępstwa *phishingu* może przebiegać w różny sposób, ale najczęściej polega na nakłonieniu użytkownika do samodzielnego wpisania poufnych danych na specjalnie spreparowanej stronie internetowej mającej imitować oryginalną stronę instytucji (np. banku internetowego, serwisu aukcyjnego, internetowego systemu płatności), pod którą podszywają się oszuści. Zazwyczaj stosowaną techniką przez *phisherów* jest wysyłanie spreparowanego listu elektronicznego, który rzekomo pochodzi np. z banku. Z treści takiego listu wynika konieczność natychmiastowego kontaktu z bankiem w celu np. odblokowania zablokowanego konta, weryfikacji danych karty płatniczej celem przedłużenia okresu jej ważności, ponowna aktywacja karty, dodanie nowej aplikacji, poprawa bezpieczeństwa dokonywanych transakcji itp. Taki e-mail zwykle zawiera link prowadzący do sfałszowanej strony. Adres jest tak podrobiony, aby ofiara myślała, że to prawdziwa strona instytucji, z którą chcemy się połączyć. W tym celu wykorzystywane są błędy w przeglądarkach lub proste triki, np. adres strony zawiera cyfrę 1 zamiast litery l[281].

[279] Gajewski M.: op. cit.
[280] Ibidem.
[281] Źródło: http://www.tp.pl/prt/pl/tpcert/bezpieczenstwo/zagrozenia/oszustwa/phishing (dostęp 31.08.2013).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 30. Przykładowy e-mail wysyłany przez *pisherów* do klientów banku PKO BP SA w maju 2014 roku

From: iPKO [mailto:serwis@internetowy-ipko.pl]
Sent: Tuesday, May 27, 2014 6:24 PM
Subject: (1) Nowa wiadomosc
Szanowny kliencie ,
Otrzymałeś nową wiadomość
Proszę clik tutaj . (link: hxxp://www.cavucci.it/pl/ipko.pl/ikds/)

Źródło: http://niebezpiecznik.pl/post/uwaga-klienci-pko-i-citi-banku-trwa-potezna-kampania-phishingowa-z-kont-skradziono-juz-kilkanascie-tysiecy-zlotych/ (dostęp 10.03.2015).

Phisherzy stosują coraz bardziej wyrafinowane techniki, przykładem może być niebezpieczny kod zaszyty w plikach graficznych, *keylogger* automatycznie pobierany w chwili otwarcia wiadomości, czy odpowiednio spreparowane strony internetowe, które w swym wyglądzie w niczym nie różnią się od oryginalnych, łącznie z tzw. kłódką bezpieczeństwa widoczną w prawym dolnym rogu okna przeglądarki Internet Explorer. *Phishing* staje się coraz bardziej wyrafinowany, co powoduje, iż coraz większa liczba osób pada jego ofiarą[282].

2.2.2. Sposób działania sprawców phishingu

Zdaniem J. Nawrata [283], wektorem ataków *phishingowych* mogą być przede wszystkim wiadomości poczty elektronicznej (tzw. e-maile), które w formie spamu rozsyłane są do potencjalnych klientów różnych serwisów (nie tylko banków internetowych, ale również serwisów aukcyjnych, serwisów finansowych, czy płatnych serwisów informacyjnych). Odpowiednio spreparowane wiadomości poczty elektronicznej (szata graficzna, forma, treść, itp.), udające oficjalne wiadomości wysłane z banku lub przez właściciela, czy administratora danego serwisu internetowego, zawierają w swej treści odwołania do fałszywych serwerów, na stronach których nieostrożni czy nieświadomi użytkownicy skłaniani są do ujawnienia danych uwierzytelniających (identyfikatorów, haseł, numerów PIN) lub/i danych potrzebnych do autoryzacji transakcji (kodów jednorazowych). Inne, często wyko-

[282] Janus R., Delio M.: op. cit.
[283] Nawrat J. 2008: Phishing i antypishing w bankowości internetowej, „Boston IT Security Review" nr 04, s. 50.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

rzystywane przez atakujących wektory ataków, to złośliwe oprogramowanie (wirusy, robaki internetowe, konie trojańskie, *spyware*, *keyloggery*, *screen--grabbery*, IRC i komunikatory podatności przeglądarek internetowych, transparentne serwery *proxy*, techniki URL *obfuscation* (komplikowanie zapisu lub kodowanie adresów URL w celu ukrycia rzeczywistych adresów serwerów lub ukrycia faktu zastosowania przekierowania) oraz korzystanie z mechanizmów wyszukiwarek internetowych. Najskuteczniejsze z ataków *phishingowych* to te, które stosują kombinację wielu wektorów w połączeniu z technikami inżynierii społecznej (*social engineering*).

Typowy atak kombinowany wykorzystuje technikę *Cross Site Scripting*[284], lecz zamiast zamieniać autentyczną stronę na spreparowaną przez oszusta, wysyłany jest e-mail z adresem URL strony, zawierający zaszyty kod. Kiedy adresat takiej wiadomości skorzysta z załączonego adresu, kod wyświetli okno logowania wyglądające na autentyczne, a w rzeczywistości przechwytujące informacje, które niezbędne są do zalogowania na danej stronie lub przekierowują użytkownika na przygotowaną przez *pishera* stronę[285].

Podstawowe ataki *phishingowe* polegają na przekierowaniu odwołań użytkowników do fałszywych stron internetowych, które jedynie udają autentyczne strony bankowe. Przez odpowiednio spreparowane formularze, przygotowane tak, aby do złudzenia przypominały strony serwera bankowości internetowej, użytkownik następnie odpytywany jest przez atakującego o dane do uwierzytelnień, o numery kart kredytowych, jednorazowe kody autoryzacyjne czy numery PIN. W zaawansowanych przypadkach atakujący posługuje się bardziej wyszukanymi metodami. Może np. używać oprogramowania złośliwego, które infekuje stacje klienta. Do infekcji często dochodzi w sposób całkowicie niezauważalny dla użytkownika, gdy ten – np. przeglądając strony internetowe – dostaje się na zainfekowane przez *phishera* strony. Oprogramowanie złośliwe może funkcjonować jako tzw. tylne wejście (*backdoor*) i rejestrator aktywności klawiatury (*keylogger*). Jego zadaniem może być śledzenie odwołania do serwisów bankowości internetowej i kiedy takie odwołania stwierdza, rejestruje i loguje aktywność klawiatury. Skutkiem tego takie dane, jak nazwy użytkowników oraz hasła dostępowe, a także ewentualnie numery PIN i kody do autoryzowania transakcji przestają

[284] Cross-site scripting (XSS) – sposób ataku na serwis WWW polegający na osadzeniu w treści atakowanej strony kodu (zazwyczaj JavaScript), który wyświetlony innym użytkownikom może doprowadzić do wykonania przez nich niepożądanych akcji. Skrypt umieszczony w zaatakowanej stronie może obejść niektóre mechanizmy kontroli dostępu do danych użytkownika. http://pl.wikipedia.org/wiki/Cross-site_scripting (dostęp 10.03.2015).

[285] Janus R., Delio M.: op. cit.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

być poufne, mimo faktu, że połączenia do systemów bankowości internetowej są szyfrowane[286].

Warto pamiętać, że złośliwe oprogramowanie wykorzystane przez sprawcę może także rejestrować zrzuty ekranowe i przez to mieć podgląd przebiegu połączenia (np. rachunki, stany kont, dane o użytkowniku). Zarejestrowany w ten sposób plik lub log, który zawiera informacje o podsłuchanej sesji przesyłany jest następnie do sprawcy w jawnej lub zaszyfrowanej z wykorzystaniem różnych kanałów transmisyjnych.

Nawrat podkreśla, iż atak *pishingowy* może być przeprowadzany na pięć różnych sposobów.

1. Phishing z wykorzystaniem wiadomości e-mail

Jest to najstarszy spośród szerokiej gamy mechanizmów ataków *phishingowych* i nadal najbardziej popularny, który polega na wysłaniu potencjalnemu klientowi odpowiednio spreparowanej wiadomości poczty elektronicznej (e-mail). W wiadomości takiej atakujący podszywa się pod bank i informuje adresata na przykład o anulowaniu przez bank ostatnio dokonanej transakcji lub o konieczności aktualizacji danych osobowych. W ten sposób atakujący usiłuje nakłonić atakowanego do kontaktu z fałszywym serwerem, który udaje serwer jego banku. W treści wiadomości e-mail podany jest odnośnik (link) do strony, gdzie użytkownik może przeprowadzić wszystkie niezbędne formalności. Na tej stronie przeważnie publikowany jest formularz z zapytaniami o dane uwierzytelniające (identyfikator, hasło dostępowe, numer PIN), o jednorazowe kody autoryzacyjne, czy o numery kart kredytowych. Warto zaznaczyć, iż przesłane wiadomości posiadają treść i wygląd bardzo zbliżony do oficjalnego szablonu korespondencji e-mail wysyłanej przez bank, a prezentowana użytkownikowi strona internetowa przypomina swą szatą graficzną oficjalne strony systemu bankowości internetowej[287], co prezentuje poniższa rycina.

[286] Nawrat J.: op. cit., s. 51.
[287] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 31. Przykład fałszywej wiadomości bankowej z listopada 2011 roku – ING Bank Śląski SA

Od: ING Bank <suppinf@ingbank.pl>
Data: 21 listopada 2011 10:01:47 CET
Do:
Temat: UWAGA : Masz 1 nowa wiadomosc!
ING
DAJEMY CI SIŁĘ LWA
UWAGA : Masz 1 nowa wiadomosc!
Zaloguj : ING BankOnLine
Dziekujemy za korzystanie z ING Bank !
ING BANK SLASKI
2011 ING Bank Slaski S.A. Wszelkie prawa zastrzezone. Korzystanie z serwisu oznacza akceptacje.
Email ID: 469810

Źródło: http://www.ingbank.pl/aktualnosci/bankowosc-elektroniczna?news_id=1000861,wyludzenie--danych (dostęp 10.03.2015).

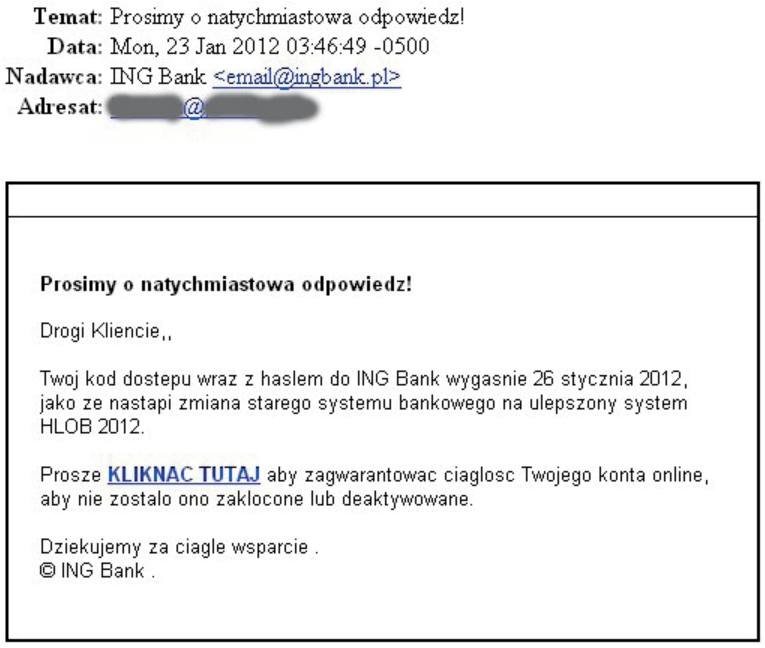
Typowe dla wiadomości e-mail wysyłanych przez atakujących są:

1) format HTML treści wiadomości (szata graficzna z logo banku, sugerująca autentyczność wiadomości, możliwość wbudowywania do wiadomości gotowych do natychmiastowego wykorzystania odnośników do stron fałszywych serwerów);
2) stosowanie obejść systemów filtracji antyspamowej;
3) komplikowanie zapisu adresów URL, do których kierowany jest atakowany klient;
4) przekłamywanie odnośników (adresów URL).

O tym, iż nie ma banku całkowicie odpornego na atak *phishingowy,* w którym sprawcy nie próbowaliby swoich szans świadczą zamieszczone poniżej ryciny, które zawierają przykłady fałszywych wiadomości przesyłanych przez przestępców klientom różnych banków.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 32. Przykład fałszywej wiadomości bankowej ze stycznia 2012 roku – ING Bank Śląski SA



Temat: Prosimy o natychmiastowa odpowiedz!
Data: Mon, 23 Jan 2012 03:46:49 -0500
Nadawca: ING Bank <email@ingbank.pl>
Adresat: [redacted]

Prosimy o natychmiastowa odpowiedz!

Drogi Kliencie,,

Twoj kod dostepu wraz z haslem do ING Bank wygasnie 26 stycznia 2012, jako ze nastapi zmiana starego systemu bankowego na ulepszony system HLOB 2012.

Prosze **KLIKNAC TUTAJ** aby zagwarantowac ciaglosc Twojego konta online, aby nie zostalo ono zaklocone lub deaktywowane.

Dziekujemy za ciagle wsparcie .
© ING Bank .

Źródło: http://www.ingbank.pl/aktualnosci/bankowosc-elektroniczna?news_id=1000950%2Cstyczen2012-phishing (dostęp 10.03.2015).

Rysunek 33. Przykład fałszywej wiadomości bankowej zawierający informację o zablokowanym dostępie do Pekao24

Bank Pekao

Twoje konto zostalo tymczasowo zablokowane.

Ze wzgledu na wiele nieudanych prób logowania do konta online konto jest czasowo zablokowane.

Kliknij ponizszy link, aby odblokowac konto:
https://www.pekao24.pl/

© 2002-2013 Bank Pekao S.A.

Źródło: http://www.pekao.com.pl/indywidualni/bankowosc_elektroniczna/Bezpieczenstwo/komunikatyibiuletyny#tab=1,paragraf1 (dostęp 17.07.2014).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 34. Przykład fałszywej wiadomości bankowej z czerwca 2013 roku – PKO BP

From: iPKO [mailto:serwis.internetowy@ipk.pl]
Sent: Thursday, June 20, 2013 3:20 PM
To: tech@serwis.wp.pl
Subject: Nowa wiadomosc !

Szanowny kliencie,

Masz nową wiadomość z iPKO Banku.
Kliknij tutaj, aby przeczytać.

Data transmisji: 20/06/2013

Źródło: http://proline.pl/?n=atak-phishingowy-na-uzytkownikow-serwisu-ipko-cyberprzestepcy--wyludzaja-dane-logowania-oraz-kody-jednorazowe (dostęp 10.03.2015).

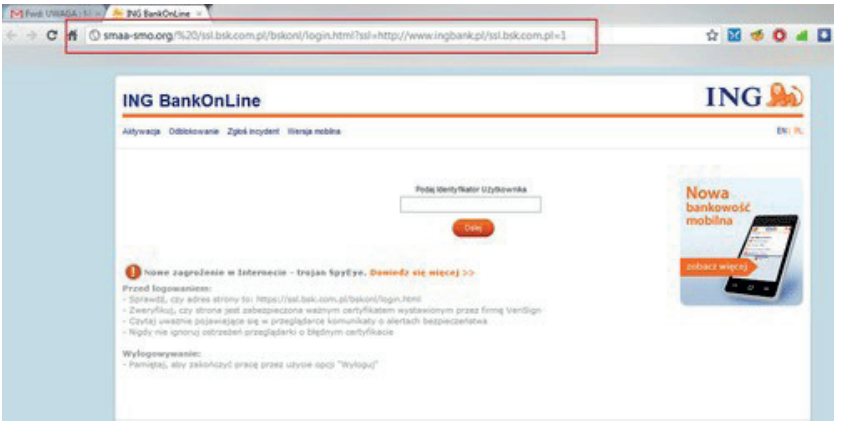
Przesłane w ten sposób wiadomości, często skonstruowane są tak, że większość zawartych w nich elementów graficznych pochodzi z legalnego serwera i jest stamtąd pobierana podczas przeglądania wiadomości przy pomocy graficznego klienta poczty lub poprzez *web-maila*. Pośród tych elementów graficznych, niewzbudzających podejrzeń atakowanego, zamieszczane są informacje, zapytania i formularze pochodzące od atakującego[288].

Na poniższych rycinach zamieszczone są przykłady fałszywych stron, na które przekierowywani byli adresaci poczty po kliknięciu w zawarte w fałszywych e-mailach linki. Zwrócić należy uwagę, iż strony te są łudząco podobne do autentycznych stron bankowych.

[288] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 35. Przykład fałszywej strony internetowej, na którą przekierowywał zamieszczony w e-mailu link z listopada 2011 roku – ING Bank Śląski SA



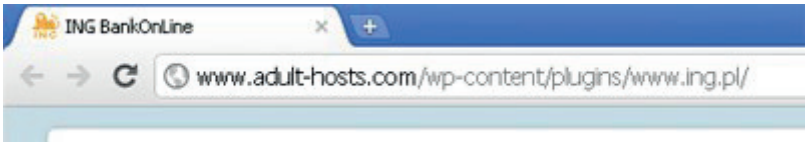
Źródło: http://www.ingbank.pl/aktualnosci/bankowosc-elektroniczna?news_id=1000861,wyludzenie--danych (dostęp 10.03.2015).

Rysunek 36. Fałszywa strona z logowaniem do rachunku bankowego (bank nigdy nie prosi o wpisanie pełnego hasła użytkownika) – ING Bank Śląski SA

ING BankOnLine
Aktywacja Odblokowanie Zgłoś incydent Wersja mobilna
Podaj hasło dla użytkownika
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
Dalej
Nowe zagrożenie w Internecie - trojan SpyEye. Dowiedz się więcej >>

Źródło: Tamże.

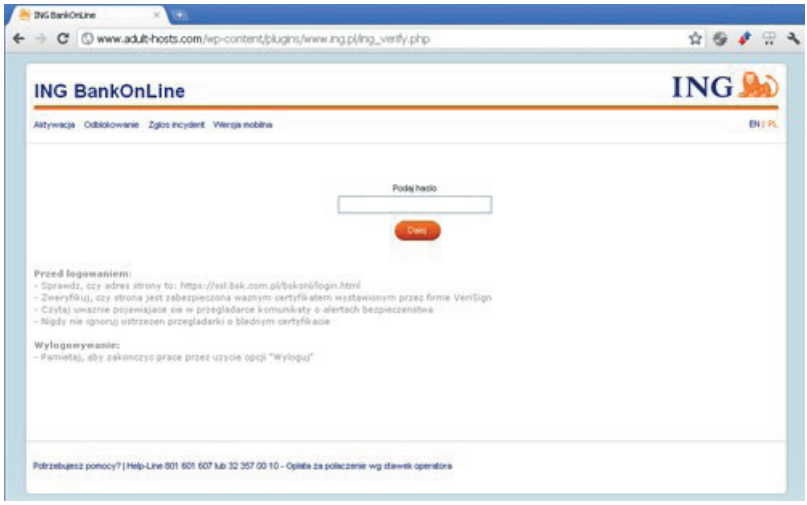
Rysunek 37. Adres strony, na którą przekierowywał fałszywy link – styczeń 2012 – ING Bank Śląski SA



Źródło: http://www.ingbank.pl/aktualnosci/bankowosc-elektroniczna?news_id=1000950%2Cstyczen2012-phishing (dostęp 10.03.2015).

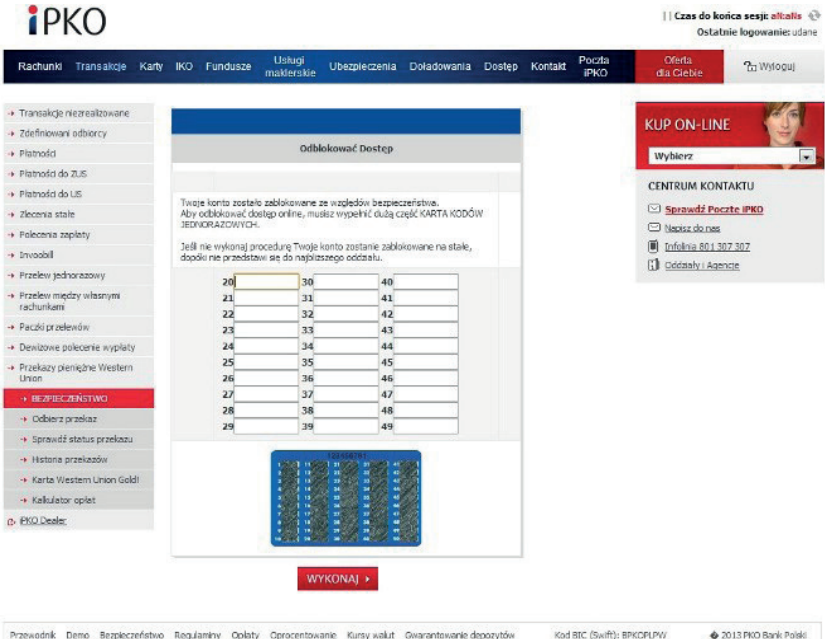
Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 38. Wygląd fałszywej strony logowania – ING Bank Śląski SA


ING BankOnLine
www.adult-hosts.com/wp-content/plugins/www.ing.pl/ing_verify.php
ING BankOnLine
ING
Aktywacja Odblokowanie Zgłoś incydent Wersja mobilna
EN | PL
Podaj hasło
Dalej
Przed logowaniem:
- Sprawdź, czy adres strony to: https://esl.bsk.com.pl/bskonl/login.html
- Zweryfikuj, czy strona jest zabezpieczona ważnym certyfikatem wystawionym przez firmę VeriSign
- Czytaj uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa
- Nigdy nie ignoruj ostrzeżeń przeglądarki o błędnym certyfikacie
Wylogowywanie:
- Pamiętaj, aby zakończyć pracę przez użycie opcji "Wyloguj"
Potrzebujesz pomocy? | Help-Line 801 601 607 lub 32 357 00 10 - Opłata za połączenie wg stawek operatora

Źródło: Tamże.

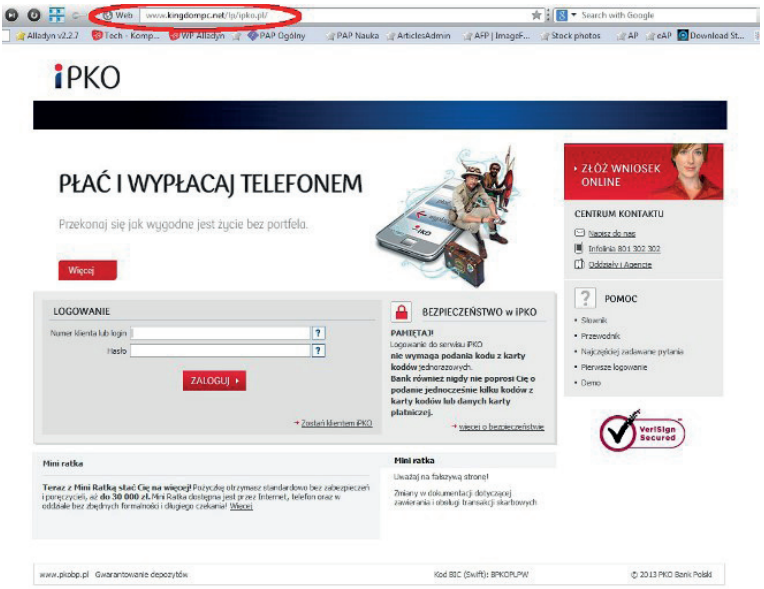
Rysunek 39. Adres fałszywej strony bankowej banku PKO BP SA



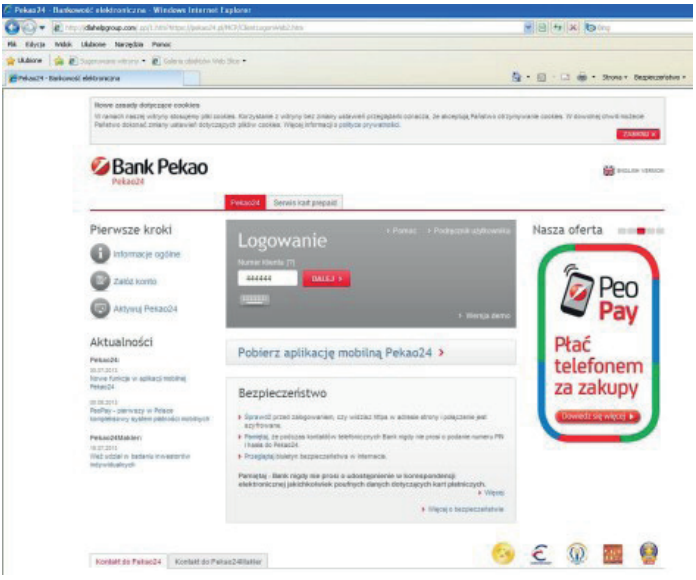
Źródło: http://proline.pl/?n=atak-phishingowy-na-uzytkownikow-serwisu-ipko-cyberprzestepcy--wyludzaja-dane-logowania-oraz-kody-jednorazowe (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 40. Fałszywa strona logowania banku PKO BP SA



Źródło: Tamże.

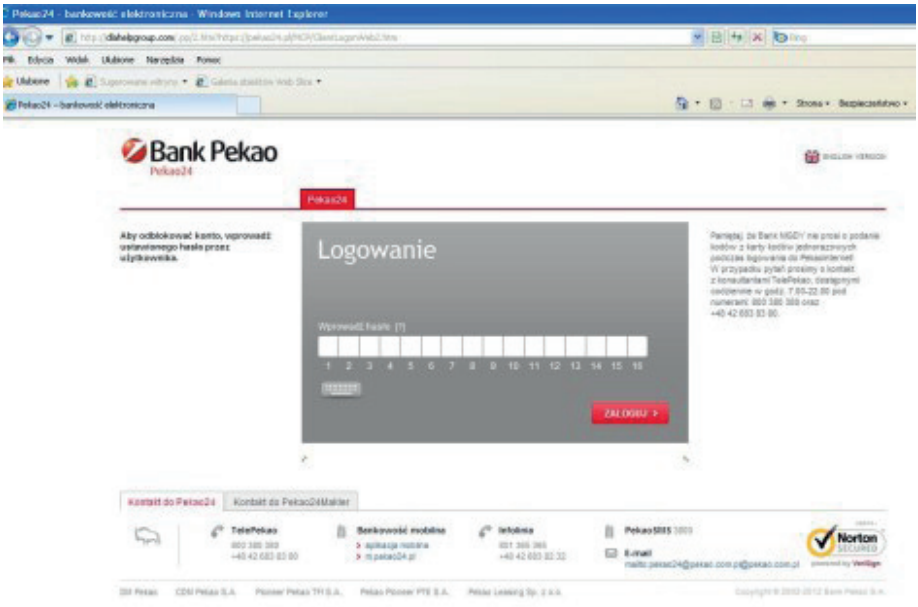


Rysunek 41. Fałszywa strona banku Pekao SA, na którą przekierowywał zamieszczony w e-mailu link

Źródło: http://www.pekao.com.pl/indywidualni/bankowosc_elektroniczna/Bezpieczenstwo/komunikatyibiuletyny#tab=1,paragraf1 (dostęp 17.07.2014).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 42. Fałszywa strona logowania do usługi bankowości internetowej



Źródło: Tamże.

2. Phishing z wykorzystaniem stron internetowych i mechanizmów usług webowych

Strony internetowe, które wykorzystywane są do przeprowadzania ataków *phishingowych*, mogą być publikowane na serwerach zarządzanych przez atakującego lub na zaatakowanych serwerach internetowych, które są własnością innych organizacji. Typowe metody przeprowadzania ataków wykorzystujących strony internetowe i mechanizmy usług webowych to:

1) zamieszczanie, często w postaci zakamuflowanej (technikami komplikowania zapisu adresów URL, określanymi też jako *URL obfuscation*), na często odwiedzanych stronach internetowych odnośników do fałszywych serwisów bankowych;
2) wykorzystanie, w charakterze graficznej reprezentacji odnośników do fałszywych stron, bannerów z elementami graficznymi charakterystycznymi dla banku, którego klienci są na celu ataków *phishingowych*;
3) wykorzystanie pozbawionych ramek okienek typu *pop-up* dla ukrycia prawdziwego adresu pochodzenia komunikatów od atakującego;

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

4) osadzanie na często odwiedzanych stronach lub na stronach, których adres, na ogół w zamaskowanej postaci, propaguje atakujący, obiektów, aktywujących w środowisku przeglądarek internetowych podatności skutkujące umożliwieniem atakującemu przejęcie zdalnej kontroli nad stacją roboczą użytkownika lub zainstalowanie dowolnego, złośliwego oprogramowania (na przykład *keylogger*, *screen-grabber*, *backdoor*, koń trojański);
5) nadużycie – zdefiniowanych w środowisku przeglądarki internetowej – relacji zaufania w celu podszycia się pod autoryzowaną domenę lub zaufany serwer uprawniony do uruchamiania określonych skryptów lub odwołań do określonych źródeł danych;
6) przeszukiwanie historii odwiedzin stron w celu spersonalizowania ataku (na przykład dostosowania formy i treści spamu *phishingowego* do konkretnego banku, z którego korzysta klient) [289].

Funkcjonuje wiele mniej lub bardziej skutecznych sposobów kamuflowania adresów stron internetowych, w taki sposób, aby wytworzyć u użytkownika błędne przekonanie, iż odwołuje się on do prawidłowego serwera bankowości internetowej.

Najbardziej banalny, zdaniem Nawrata, sposób polega na rejestrowaniu i stosowaniu nazw domen, które przypominają domeny serwisów bankowości internetowej (na przykład domena www.ing.pl, może przybrać postać www.ing.com.pl). Inny, równie trywialny, to odwołanie w odnośniku do podstawionego serwera poprzez adres IP zamiast poprzez nazwę (adres może wzbudzać mniejsze podejrzenia użytkownika niż odpowiadająca mu nazwa serwera). Jeszcze innym sposobem, poprzez który atakujący stwarza wrażenie, że przesyłany użytkownikowi adres URL wskazuje na legalny serwis bankowości internetowej, jest wykorzystanie subdomen[290]. Atakujący rejestruje domenę na przykład DOMENA.COM, a do celów *phishingowych* stosuje adres WWW.BANK.COM.DOMENA.COM. Wreszcie użytkownik serwisu www.bank.com może zostać przez atakującego wprowadzony w błąd następującym sposobem zapisu adresu URL:

[289] Ibidem.
[290] Subdomena – to adres internetowy przynależący do właściwej domeny. Jest to powszechnie dostępna usługa wymagająca uzgodnienia z administratorem serwera wirtualnego, lub właściciela domeny. Praktycznie wygląda to tak, że posiadając domenę www.agp.pl i zamierzamy otworzyć w tej domenie serwis internetowy o tematyce Mazury, zakładamy w tym celu subdomenę www.mazury.agp.pl. Źródło: http://www.webreklama.pl/informator/domeny/Subdomena.html (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

- https://www.bank:com@<adres_IP_podstawionego_serwera>/<ścieżka_do_strony_www>.

Przykładowo, jeśli adres IP 172.16.1.100 odpowiada podstawionemu serwerowi, to odnośnik do strony może wyglądać tak:

- https://www.bank:com@172.16.1.100/login_page.html[291].

Prostą metodą ataku *phishingowego* jest również publikowanie w postaci graficznej odnośników do fałszywych serwerów bankowości internetowej. Grafika reprezentująca odnośnik najczęściej pochodzi z legalnego serwera banku, którego klienci są celem ataków. Atakowani klienci przeważnie nie sprawdzają, jaki odnośnik kryje się pod zaprezentowaną grafiką, która budzi ich zaufanie. Jeśli atakującemu uda się przejąć kontrolę nad połączeniem od użytkownika , przejąć kontrolę nad stacją użytkownika (na przykład stosując złośliwe oprogramowanie) lub też w skrajnym przypadku wykorzystać podatności aplikacji systemu bankowości internetowej na wszelkie formy iniekcji kodów i XSS (*cross site scripting*), może on generować w przeglądarce atakowanego pozbawione ramek okienka (na przykład z żądaniem podania haseł, kodów autoryzacyjnych czy numerów kart kredytowych) i jednocześnie skutecznie ukrywać prawdziwy adres pochodzenia komunikatów związanych z atakiem[292].

3. Phishing z wykorzystaniem złośliwego oprogramowania

Złośliwe oprogramowanie może być przez atakującego wykorzystane na dwa sposoby:

1. Infekowanie stacji użytkowników, wykorzystywanych następnie do celów dystrybucji stacherskich wiadomości poczty lub innego rodzaju komunikatów (przez IRC lub komunikatory internetowe) albo też infekowania innych stacji. Zainfekowana stacja staje się elementem bonetu (na ogół bardzo licznego zbioru zainfekowanych stacji), nad którym kontrolę sprawuje jego atakujący.
2. Przeprowadzania ataków *phishingowych* sprowadzających się do infekowania końcowych stacji użytkowników w celu przechwytywania potwierdzeń tożsamości użytkownika (identyfikatory, hasła) w systemach bankowości internetowej, danych służących do autoryzacji dokonywanych przez użytkownika transakcji (jednorazowe kody autoryzacyjne) i innych ważnych danych (numery kart kredytowych)[293].

[291] Nawrat J.: op. cit., s. 52.
[292] Ibidem.
[293] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Sprawcy najczęściej posługują się w tym celu „trojanami" (nazwa pochodzi od konia trojańskiego) i programami szpiegującymi. Nie sposób w tym miejscu wymienić wszystkich programów oraz sposobów ich działania. Najbardziej znane programy tego typu, to *Trojan-Spy.html*, *Trojan.Win32.Qhost* oraz *Trojan.Win32.DNSChanger*. Ten pierwszy ma wiele wariacji, a każda z nich dotyczy innego banku/instytucji (wtedy do głównej nazwy dodawana jest informacja kojarząca tego „trojana" z konkretną firmą)[294].

4. *Phishing* z wykorzystaniem usługi IRC i komunikatorów internetowych

IRC[295] oraz komunikatory internetowe IM[296] to kolejny wektor ataków *phishingowych*. Ciągły rozwój tej kategorii oprogramowania, oferującego już możliwości łatwego przesyłania treści takich jak odnośniki HTML, pliki multimedialne, grafiki, programy oraz inne obiekty binarne, skutkuje niestety także możliwością wykorzystania usług IRC i komunikatorów do przeprowadzania ataków *phishingowych* o mechanizmach analogicznych jak te, dla których kanałem dystrybucji są usługi webowe[297].

5. Phishing realizowany za pośrednictwem ataków *man–in–the–middle*[298]

Ataki *man-in-the-middle* skierowane są na połączenia realizowane przez użytkownika do serwerów bankowości internetowej. Celem ich jest naruszenie poufności danych transmitowanych przez użytkownika, w tym zwłaszcza – w przypadku *phishingu* – danych potwierdzających tożsamość użytkownika lub stanowiących podstawę autoryzacji dokonywanych przez niego transakcji. Atak tego typu polega na interaktywnej komunikacji

[294] Ziarek M.: Phishing, pharming i sieci zombie i to czego nie wiesz o swoim komputerze, 14.07.2009, http://www.trochetechniki.pl/Phishing%2C-pharming-i-sieci-zombie--to-czego-nie-wiesz-o-swoim-komputerze,t,604,page,1.html (dostęp 10.03.2015).

[295] IRC (ang. Internet Relay Chat) – jedna ze starszych usług sieciowych umożliwiająca rozmowę na tematycznych lub towarzyskich kanałach komunikacyjnych, jak również prywatną z inną podłączoną aktualnie osobą. http://pl.wikipedia.org/wiki/Internet_Relay_Chat (dostęp 10.03.2015).

[296] IM – (ang. Instant Messenger – natychmiastowa komunikacja) – program pozwalający na bezpośrednie komunikowanie się przez Internet lub sieć lokalną za pomocą wiadomości tekstowych, głosowych lub przekazów multimedialnych. http://www.i-slownik.pl/1736,komunikator-internetowy-lub-instant-messenger-im/ (dostęp 10.03.2015).

[297] Nawrat J.: op. cit., s. 52.

[298] Ataki Man in the Middle (w skrócie MITM) stanowią zagrożenie dla każdej, nawet szyfrowanej komunikacji typu klient – serwer. Koncepcja tego ataku przewiduje podsłuch i przejęcie połączenia, nawet w przypadku braku możliwości złamania stosowanego przez strony komunikacji algorytmu szyfrowania. Szczególnie częstym przedmiotem ataków MITM są szyfrowane sesje SSH (Secure Shell) i SSL (Secure Sockets Layer), które służą do przesyłania często bardzo istotnych i poufnych informacji. http://www.poradykomputerowe.pl/porady_komputerowe/bezpieczenstwo_informacji/ataki_man_in_the_middle-306.html (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

przestępcy z klientem i wykorzystaniu wyłudzonych informacji w czasie rzeczywistym[299].

W arsenale środków pozostających do dyspozycji atakującego są następujące techniki:

1) transparentne *proxy*;
2) przekłamanie zawartości buforów serwisu nazw (DNS *cache poisoning*[300]), przejmowanie domen, fałszowanie lokalnych plików *hosts*;
3) przekłamania, kamuflaż lub komplikowanie zapisu adresów URL;
4) rekonfiguracja ustawień *proxy* przeglądarek internetowych na stacjach roboczych użytkowników;
5) przekierowania portów[301].

Atak *man-in-the-middle* wykorzystuje dodatkowy serwer, który łączy klienta z serwerem docelowym. Jego ideą jest przejmowanie pakietów, ich modyfikacja i wykorzystywanie w celu osiągnięcia własnych korzyści. W praktyce atak ten jest trudny do wykrycia, zwłaszcza po stronie użytkownika. Atakujący może nie tylko przechwycić pakiety, ale także wykradać informacje, przechwycić aktualną sesję i dowolnie ją modyfikować. Większość działań opiera się na *sniffingu* (podsłuchu). Pewnym minusem w stosunku do „typowego" *phishingu* jest fakt, że nie można go stosować masowo. O ile wysyłając maile ze sfałszowanymi stronami atakujący otrzymuje wiele numerów kont i haseł, o tyle w tego rodzaju ataku musi się skupić na jednym, ewentualnie kilku klientach, którzy w dodatku niekoniecznie muszą na koncie mieć sumę rekompensującą wysiłek włożony w tego typu atak. Dlatego właśnie atak typu *man-in-the-middle* najczęściej stosuje się w celu kradzieży tożsamości i danych[302].

Atak typu *man–in-the-middle* umożliwia atakującemu przechwycenia lub podsłuchania szyfrowanej sesji – połączenie klienta z bankiem internetowym – co sprawca może osiągnąć poprzez podsunięcie klientowi sfałszowanego certyfikatu uwierzytelniającego podrobione strony (np. strona internetowa banku) i sfałszowanego odwzorowania DNS. Podkreślić należy, iż nie dochodzi w tym wypadku do jakiegoś nadzwyczajnego oddziaływania

[299] Szwajkowska G. i in.: op. cit., s. 35.

[300] Zatruwanie DNS (ang. cache poisoning) – technika phishingu polegająca na wysłaniu przez atakującego do serwera DNS fałszywej informacji kojarzącej nazwę domeny z adresem IP. Serwer DNS zapamiętuje ją na pewien czas (do kilku godzin) i zwraca klientom zapamiętany adres IP, czego skutkiem jest przeniesienie na fałszywą stronę. http://pl.wikipedia.org/wiki/Zatruwanie_DNS (dostęp 01.09.2013).

[301] Nawrat J.: op. cit., s. 53.

[302] Ziarek M.: op. cit.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

na system informatyczny banku, atakujący podłącza się do niego jak zwykły klient. Nie dochodzi również do oddziaływania na system informatyczny ofiary, do którego sprawca przesyła jedynie sfałszowaną informację, która ma na celu uwierzytelnienie atakującego jako banku, czyli oszukanie użytkownika i późniejsze skorzystanie z jego identyfikatora i hasła. Atak tego typu jest atakiem aktywnym, o wysokiej szkodliwości, który jest używany bardzo często w różnych odmianach do kradzieży dużych sum pieniędzy[303].

Zbliżoną do *phishingu* realizowanego za pośrednictwem ataków *man-in-the-middle* jest metoda *man-in-the-browser*. W tym wypadku atak *phishera* skierowany jest przeciwko przeglądarce internetowej klienta banku i polega na modyfikowaniu danych, które wpisywane są przez klienta banku w formularzach podczas korzystania z usług bankowości internetowej. Złośliwy kod, który dokonuje modyfikacji zazwyczaj zapisuje się na dysku twardym komputera klienta i profilowany być musi pod kątem określonego systemu bankowości internetowej[304]. Jak zatem można wywnioskować, w przypadku ataku tego typu, główny ciężar przeciwdziałania mu spoczywa właśnie na banku.

Również klient banku może przyczynić się do przeciwdziałania atakom typu *man-in-the-browser*. Powinien on w tym celu odpowiednio, zgodnie z zaleceniami banku, skonfigurować przeglądarkę internetową, z której korzysta do kontaktów za bankiem w ramach usług bankowości internetowej, a także na bieżąco ją aktualizować. Powinien również zainstalować, odpowiednio skonfigurować i na bieżąco aktualizować oprogramowanie antywirusowe. Warto zauważyć, iż niektóre programy antywirusowe, jak chociażby Kaspersky Internet Security 2014, poza filtrem antyphishingowym, zawierają również technologię „bezpiecznych pieniądzy", gwarantującą, zdaniem Kaspersky Lab, maksymalną ochronę bankowości elektronicznej i transakcji płatniczych on-line. Klient banku powinien również okresowo kontrolować wyciągi bankowe lub historii rachunku[305].

Odmiennym, niż przesyłanie wiadomości e-mail zawierających link odsyłający na fałszywe strony bankowe, sposobem dokonywania przestępstwa *phishingu* jest przesyłanie klientowi banku, za pośrednictwem poczty, przesyłki zawierającej CD lub inny nośnik danych przeznaczony do użytku w komputerze. Nośnik taki oznaczony jest stosowną grafiką zawierająca

[303] Szmit M., Politowska I. 2007: O artykule 267 Kodeksu Karnego oczami biegłego, CBKE e-biuletyn, 03.09.2007.
[304] Szwajkowska G. i in.: op. cit., s. 36.
[305] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

logo banku i inne tego typu elementy mające wskazywać jego oryginalne pochodzenie. Na nośniku znajduje się informacja, iż może ona zostać wykorzystana w komputerze w celu zapoznania się z najnowszą ofertą banku lub obejrzenia filmu. W rzeczywistości po włożeniu nośnika do czytnika w komputerze, uruchamia się złośliwe oprogramowanie służące do wykradania danych. Wykradzione w ten sposób dane, przesyłane są następnie przestępcy za pośrednictwem Internetu[306].

2.2.3. Przeciwdziałanie *pishingowi*

Zanim odpowiemy na pytanie jak skutecznie bronić się przed *phishingiem*, i co najważniejsze, czy w ogóle istniej skuteczny środek ochrony przed tego typu atakami, spróbujemy podnieść kwestię odpowiedzialności za *phishing* w polskim ustawodawstwie karnym.

Mechanizm *phishingu* polega na tym, iż sprawca wysyłając do swojej potencjalnej ofiary e-mail z linkiem przekierowującym do fałszywej strony banku, wprowadza go w ten sposób w błąd, a jego celem jest uzyskanie poufnych danych dotyczących możliwości zalogowania się w internetowej witrynie banku i dokonanie nieuprawnionej wypłaty pieniędzy. A zatem działanie sprawcy (w przypadku ataków na klientów bankowości internetowej) polega na ingerencji w dane informatyczne, a celem tego działania jest osiągnięcie korzyści majątkowej – tym samym sprawca swoim zachowaniem wyczerpuje znamiona czynu określonego w art. 287 § 1 k.k. („Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych*"*), zagrożonego karą pozbawienia wolności od 3 miesięcy do lat 5. Zatem mamy w tym wypadku do czynienia z oszustwem komputerowym. Podobnie jak w przypadku *pharmingu*, który jest subtelniejszą i bardziej skomplikowaną odmianą *phishingu*.

Kluczowym pojęciem dla przestępstwa opisanego w art. 287 § 1 k.k. są dane informatyczne. Za dane informatyczne, zgodnie z brzmieniem art. 1 lit. b konwencji o cyberprzestępczości z dnia 23 listopada 2001 roku, uznaje się: „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny".

[306] Kaszubski R., Obzejta Ł.: op. cit., s. 402.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Oszustwo komputerowe określone w art. 287 § 1 k.k. jest przestępstwem kierunkowym, którego strona podmiotowa polega na działaniu w celu osiągnięcia korzyści majątkowej albo wyrządzenia szkody innej osobie, na co zwraca uwagę również Marek[307].

Ciekawość może budzić fakt, iż, zdaniem prokuratury, czyn polegający na podrobieniu strony internetowej, w celu wyłudzenia haseł i loginów dostępowych do kont bankowych, czyli *phishing*, można oceniać wyłącznie pod kątem przełamania szczególnego zabezpieczenia danych, czyli art. 267 § 1 k.k., aczkolwiek sprawcy jakichkolwiek zarzutów i tak nie można postawić, ponieważ użytkownicy korzystający z jego fałszywej strony internetowej, wprawdzie zmyleni wyglądem strony, jednakże dokonywali logowań dobrowolnie – nie można więc mówić o bezprawnym uzyskaniu informacji przez sprawcę. Wobec braku ustawowych znamion czynu zabronionego sprawa została umorzona (na podstawie art. 17 § 1 pkt 2 k.p.k.)[308].

Według danych zgromadzonych przez CERT Polska[309], w roku 2013 odnotowanych zostało 9991 zgłoszeń dotyczących *phishingu* w polskich sieciach, dotyczących 7886 adresów URL w 3.780 domenach, hostowanych na 1578 adresach IP[310]. Niemal wszystkie strony *phishingowe* były efektem włamania, a nie wykupienia usługi specjalnie w celu przestępczym. Dla porównania w roku 2012 do CERT Polska zgłoszono 5335 przypadków *phishingu* w polskich sieciach. Dotyczyły one 2576 adresów URL w 1026 domen, w tym 673 z końcówką „.pl"[311].

Zatem w roku 2013 zgłoszono o 4656 przypadków *phishingu* więcej, niż w roku 2012. Więcej, o 5310 było adresów URL, a także o 2754 domeny.

Warto pamiętać, że atakujący dysponują różnorodnym arsenałem środków technicznych do przeprowadzania ataków. Nie istnieje jedna, prosta reguła postępowania dla użytkownika, która uchroniłaby go przed wszystkimi, potencjalnie możliwymi atakami *phishingowymi*. Wprawdzie dostępne są wszelkiego rodzaju filtry *antyphishingowe* (programy sprawdzające strony internetowe odwiedzane przez użytkownika w bazie danych zawierającej wierzytelne i *phishingowe* strony internetowe), których zadaniem jest

[307] Marek A.: op. cit., s. 559.

[308] Źródło: http://olgierd.bblog.pl/wpis,prokuratura;nie;ma;takiego;przestepstwa;jak;phishing,41059.html (dostęp 10.03.2015).

[309] Zespół działający w ramach Naukowej i Akademickiej Sieci Komputerowej, który zajmuje się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie.

[310] Raport CERT Polska za 2013 rok, s. 54-55. http://www.cert.pl/PDF/Raport_CP_2013.pdf (dostęp 10.03.2015).

[311] Raport CERT Polska za 2013 rok, s. 26. http://www.cert.pl/PDF/Raport_CP_2012.pdf (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

alarmowanie użytkownika, jeśli strona, na którą ma wejść, jest znaną stroną *phishingową* lub może stanowić poważne zagrożenie dla jego bezpieczeństwa, to jednak *phishing* jest odporny na wszystkie tego typu zabezpieczenia, poza przysłowiowym zdrowym rozsądkiem.

Należy zdać sobie sprawę z faktu, że bank lub jakakolwiek instytucja, z którą mieliśmy w przeszłości do czynienia nie będzie nas prosiła o żadne dane osobowe. Na stronach banku umieszczane są komunikaty, iż bank nigdy nie wysyła e-maili z prośbą o podanie danych niezbędnych do zalogowania się na swej witrynie internetowej, ani też pełnego hasła logowania do konta. Tym bardziej za pośrednictwem niezabezpieczonych kanałów, a do takich należy właśnie poczta elektroniczna (e-mail) czy komunikatory internetowe. Należy pamiętać również o aktualizacji programów typu *internet security* (np. Kaspersky IS, czy Symantec Norton IS), które standardowo wyposażone są w funkcje *antyphishingowe*. Czasami też wystarczy dokładniej przyjrzeć się paskowi adresu strony internetowej, bo być może adres strony różni się zdecydowanie od prawidłowego adresu banku (np. zamiast *www.nazwabanku.pl* może być *www.nazwabanku.com.pl*).

Pamiętać należy również, iż zatrzymanie sprawcy *phishingu* w praktyce jest bardzo skomplikowane. Przeważnie fałszywe strony internetowe istnieją zaledwie kilka godzin. Poza tym odpowiedzi na pytanie, kto jest oszustem jest kilka. *Pisherem* może być właściciel danej strony internetowej, ale równie dobrze może nim być nieuczciwy webmaster albo właściciel serwera, a może jedynie ktoś, kto miał dostęp do serwera. Może być również tak, że tylko jego DNS został przejęty przez hackerów[312].

Zdaniem Nawrata z Biura Bezpieczeństwa Informacji i Systemów Informatycznych Raiffeisen Bank Polska SA, skuteczna obrona przed *phishingiem*, jak zwykle, polega na kompleksowym zastosowaniu kombinacji różnych środków zaradczych. Podstawowym sposobem przeciwdziałania *phishingowi* jest, jego zdaniem, edukacja użytkowników. Powinni oni dobrze znać zasady bezpiecznego korzystania z usług bankowości internetowej. Zasady te powinny być publikowane na stronie internetowej banku z panelem logowania. Dodatkowe, bardziej szczegółowe informacje, należy udostępniać użytkownikom po zalogowaniu do systemu. Wymaga podkreślenia, że edukacja użytkowników bankowości internetowej powinna być procesem ciągłym[313].

[312] Zob. http://www.oszustwsieci.pl/phishing.php (dostęp 10.03.2015).
[313] Nawrat J.: op. cit., s. 53.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

W chwili obecnej w Polsce występują dobre zabezpieczenia kont użytkowników. Większość banków wyposaża użytkowników swoich kont internetowych w tzw. tokeny[314], hasła jednorazowe/SMS-owe oraz inne formy uwierzytelniania, nigdy nie wymagają podania kompletnego hasła dostępu do konta, a jedynie jego wybrany fragment. Niektóre banki również, jak choćby Inteligo sugerują użytkownikom podczas logowania użycie innej przeglądarki do czasu załatania tej dziurawej.

Rysunek 43. Token generujący jednorazowe hasła

Źródło: http://tech.wp.pl/kat,1009785,title,Masz-konto-z-tokenem-Mozesz-stracic-wszystkie-pieniadze,wid,13245173,wiadomosc.html (dostęp 10.03.2015).

Rysunek 44. Karta kodów jednorazowych, popularna zdrapka, jako aplikacja w telefonie komórkowym

Źródło: http://myapple.pl/content/763-bank-inteligo-przyjazny-dla-klientow-z-iphone-ami.html (dostęp 10.03.2015).

[314] Token jest urządzeniem kryptograficznym, wyglądem przypominającym niewielki kalkulator, zabezpieczającym operacje dokonywane przez Internet. Token generuje hasła jednorazowe, które wyświetlane są w formie ciągu cyfr, który zmienia się co 60 sekund. Dana kombinacja cyfr jest ważna jedynie przez czas jej wyświetlania. Ciąg cyfr jest funkcją tajnego klucza zapisanego w karcie oraz aktualnego czasu. System internetowy potrafi ustalić poprawność ciągu cyfr wygenerowanego przez token. Jednorazowe hasła wytwarzane przez token wymagane są przy potwierdzaniu dokonywanych transakcji. Źródło: http://direct.money.pl/poradnik_finansowy/co;to;jest;token,poradnik;finansowy,haslo,81.html (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Środki techniczne stosowane w ochronie *antyphishingowej* można podzielić na dwie kategorie, przyjmując za kryterium podziału miejsce ich implementacji – środki techniczne do zastosowania po stronie klienta i środki techniczne do zastosowania po stronie serwera. Techniczne środki zaradcze – implementowane po stronie klienta – mają na celu zabezpieczenie stacji roboczej użytkownika oraz zwiększenie bezpieczeństwa środowiska przeglądarek internetowych. Rola banku w tym procesie polega głównie na uświadomieniu klientowi, jakie powinien on zastosować rozwiązania w celu osiągnięcia optymalnego poziomu bezpieczeństwa. Ważnym zaleceniem dla użytkownika jest, aby łączyć się z bankiem wyłącznie z zaufanych stacji roboczych. W praktyce sprowadza się to do korzystania z tych stacjonarnych komputerów PC, czy laptopów, do których użytkownik ma wyłączny dostęp lub które wykorzystywane są przez niewielkie grono zaufanych osób (na przykład rodzina)[315].

Stacja robocza powinna posiadać zainstalowaną najnowszą dostępną wersję przeglądarki internetowej oraz oprogramowanie zabezpieczające, na które składa się program antywirusowy, oprogramowanie antyszpiegowskie i osobisty *firewall*. Wymagania te spełniają dostępne na rynku programy komputerowe typu *internet security* (np. Kaspersky IS, Symantec Norton IS,). Przeglądarka internetowa powinna też zostać w odpowiedni sposób skonfigurowana (między innymi: wyłączona obsługa wyskakujących okienek *pop-up*, jeśli to możliwe – wyłączenie wirtualnej maszyny Javy, wyłączenie obsługi skryptów ActiveX, wyłączenie opcji *auto-play* dla plików multimedialnych, włączenie kontroli *cookies*, zabezpieczenie przed automatycznym uruchamianiem pobranych plików wykonywalnych)[316]. Nadmienić należy, iż współczesne oprogramowanie antywirusowe spełnia należycie swoje funkcje, jeśli działa w trybie permanentnej aktywności i kontroluje wszystkie pliki kopiowane na dysk i do pamięci, nie tylko z nośników takich, jak dyskietki, płyty CD/DVD, pamięć flash USB, itp., ale także poprzez interfejs sieciowy komputera. Ważnym jest również, aby system operacyjny wykorzystywany w komputerze posiadał wszystkie zalecane przez producenta łatki bezpieczeństwa, czyli zabezpieczenia wykrytych podatności na ataki. Wymóg ten jest realizowany przez instalację na bieżąco poprawek bezpieczeństwa, w miarę jak te udostępniane są przez producenta systemu operacyjnego. Na bieżąco powinny być także aktualizowane bazy oprogramowania antywirusowego i bazy sygnatur oprogramowania antyszpiegowskiego. Regularnie, nie

[315] Nawrat J.: op. cit., s. 53-54.
[316] Ibidem, s. 54.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

rzadziej jednak niż raz na tydzień, należy przeprowadzić pełne skanowanie systemu operacyjnego w celu wykrycia ewentualnych wirusów lub oprogramowania szpiegującego[317].

Niezmiernie ważnym jest, aby wykonując połączenia z bankiem internetowym korzystać z zaufanych komputerów, jest to niezwykle istotne z punktu widzenia bezpieczeństwa haseł, kodów autoryzacyjnych i samego procesu uwierzytelnień użytkownika. Zdarzają się takie sytuacje, że użytkownik zmuszony jest do skorzystania z konta bankowości internetowej, mając do dyspozycji jedynie komputer, któremu nie można do końca zaufać (na przykład w kawiarence internetowej). W takiej sytuacji po poprawnym zamknięciu połączenia przez wylogowanie się i zamknięcie okna przeglądarki, bank powinien zalecić natychmiastowy kontakt z centrum telefonicznym i żądanie zablokowania dostępu do konta. Odblokowanie konta powinno nastąpić dopiero po ponownym, uwierzytelnionym zgłoszeniu użytkownika do centrum telefonicznego i zmianie hasła dostępowego[318].

Wydaje się, że najlepszym obecnie sposobem ochrony przed kradzieżą danych potwierdzających tożsamość, jest zastosowanie metod uwierzytelnień wieloaspektowych, opartych na przykład na tokenach sprzętowych lub SMS-tokenach i zastąpienie nimi aktualnie stosowanych uwierzytelnień statycznymi hasłami. Uwierzytelnienia tokenowe bazują na schemacie uwierzytelnień wieloaspektowych. Do poprawnego uwierzytelnienia użytkownika wymagany jest aspekt wiedzy (PIN znany tylko użytkownikowi) oraz aspekt posiadania (kod wyświetlany w danym momencie na ekranie karty tokenowej, generowany na nowo, w cyklach, np. co 60 sekund). Bezpieczeństwo uwierzytelnień wieloaspektowych oparte jest na fakcie, że ani sam aspekt wiedzy (PIN), ani też sam aspekt posiadania (kod tokena), nie wystarczają do przeprowadzenia zakończonego sukcesem uwierzytelnienia użytkownika. O bezpieczeństwie uwierzytelnień tokenowych decyduje też możliwość wyłącznie jednokrotnego wykorzystania kodu tokena. Z tego powodu uwierzytelnienia tego typu są bardzo odporne na *phishing*. Podsłuch wieloaspektowych uwierzytelnień tokenowych nie skutkuje naruszeniem bezpieczeństwa dostępu[319].

Jako przykład innego rozwiązania, nie tak skutecznego, jak uwierzytelnienia wieloaspektowe, jest zastosowanie klawiatury ekranowej, którą klient posługuje się zamiast klawiaturą sprzętową przy wprowadzaniu swojego hasła. Klawiatura ekranowa wyświetlana jest w panelu logowania, a jej

[317] Ibidem.
[318] Ibidem.
[319] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

obsługa możliwa jest wyłącznie przy pomocy myszki. Klawiatura ekranowa chroni klienta przed ujawnieniem hasła dostępowego na skutek działania *keyloggera*[320]. Klawiatura ekranowa stanowi standardowe wyposażenie funkcjonujących obecnie na rynku systemów operacyjnych MS Windows, jest w nią również zaopatrzone oprogramowanie Kaspersky Internet Security. Klawiatura ekranowa wykorzystywana jest do logowania w serwisie internetowym m.in. ING Bank Śląski SA. Warto jest z niej korzystać każdorazowo podczas jakiegokolwiek logowania na stronach internetowych.

Dużą skutecznością ochrony przed atakami *phishingowymi* charakteryzowałby się system uwierzytelnień dwuaspektowych, który łączyłby statyczne hasło, wprowadzane z poziomu klawiatury ekranowej z kodem w wiadomości SMS, przesyłanym przez bank na zarejestrowany przez klienta telefon komórkowy. Klient otrzymywałby kod po zatwierdzeniu wprowadzania hasła. Pewien poziom ochrony przed *phishingiem* zapewnia system uwierzytelnień wymagający od użytkownika wprowadzenia wyłącznie wybranych znaków hasła, tzw. hasło maskowane. Dla każdego kolejnego logowania sekwencja wymaganych liter jest wyznaczana losowo[321].

Ziarek z Kaspersky Lab Polska uważa, że nigdy nie zabezpieczymy się w 100 procentach, przed atakami typu *phishing*, jednak obecnie istnieje wiele metod walki z opisanymi wyżej procederami. Podaje także kilka istotnych uwag, o których powinny pamiętać osoby korzystające z bankowości internetowej. Oto one:

1. Zazwyczaj maile wysyłane są masowo (spam), więc niemożliwe jest kierowanie zapytania do konkretnego użytkownika. Maile są w postaci bezosobowej, jeżeli bank zdecydowałby się na pisanie do nas, z pewnością użyłby formy grzecznościowej z imieniem i nazwiskiem.
2. Na komputerze powinien znajdować się program antywirusowy, a najlepiej pakiet *internet security*, w skład którego wchodzi filtr antyphishingowy.
3. Nie klikaj podejrzanie wyglądających wiadomości, nigdy nie pobieraj oprogramowania, które jest zalecane w mailach.
4. Do łączenia się z bankiem używaj protokołu SSL oraz sprawdzaj autentyczność i datę utraty ważności certyfikatów.
5. Aktualizuj system i przeglądarki internetowe.

[320] Ibidem, s. 55.
[321] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

6. Maile pochodzące od znanych firm i instytucji są podpisane cyfrowo, sprawdzaj autentyczność wiadomości, zanim przejdziesz na daną stronę[322].

2.3. Pharming

2.3.1. Pojęcie i geneza pharmingu

Pharming, zdaniem Kaszubskiego i Obzejty, jest najtrudniejszą do wykrycia formą *phishingu.* Przestępstwo to polega na przekierowaniu użytkownika bankowości internetowej z autentycznej strony banku na stronę stworzoną przez przestępców. W ten sposób osoba zamierzająca skorzystać ze strony internetowej swojego banku, na której zamierza podać dane dotyczące swojego rachunku lub karty płatniczej, wpisując adres internetowy strony, zostaje przekierowana na stronę wygenerowaną przez przestępców[323]. Nie trzeba dodawać, że strona ta łudząco przypomina stronę autentyczną.

Pharming, jest bardziej zaawansowaną i niebezpieczną dla użytkownika odmianą *phishingu*. Cel w przypadku obu przestępstw jest ten sam – wyłudzenie poufnych danych osobistych. Różnica natomiast polega na tym, że w przypadku *pharmingu* nie jest wysyłana informacja nakłaniająca użytkownika do podania swoich poufnych informacji, zaś w momencie odwiedzania przez użytkownika witryny internetowej (np. strony internetowej swojego banku) następuje niezależne od wiedzy i udziału użytkownika przekierowanie połączenia do fałszywej strony cyberoszusta, zamiast na właściwą stronę, mimo, że użytkownik wpisał prawidłowy adres strony. Jednym słowem *pharming* polega na przekierowaniu użytkownika Internetu do spreparowanej strony internetowej, która wyglądem może przypominać (może być wręcz identyczna) witrynę banku internetowego, serwisu aukcyjnego, sklepu internetowego czy innej instytucji, która hakerowi może przynieść korzyści finansowe**.** Strony takie tworzone są najczęściej w celu zdobycia danych, takich jak login, hasło, numer karty kredytowej, PIN i innych – mogą one zostać wykorzystane do dokonania kradzieży pieniędzy z konta bankowego[324].

[322] Ziarek M.: op. cit.
[323] Kaszubski R., Obzejta Ł.: op. cit., s. 402-403.
[324] Jeleśniański M. 2006: Pharming – nadchodzi nowe zagrożenie?, artykuł z dnia 04.02., http://pccentre.pl (dostęp 31.08.2013).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Geneza pojęcia „pharming" wiązana jest ze słowem „farming", albowiem w subkulturze hakerskiej popularne jest zamienianie w wyrazach „f" na „ph". Sprawca bowiem „zbiera żniwo" swojej działalności w postaci poufnych danych[325] lub też „troszczy" się o szereg przynoszących mu zysk serwerów, jak o zwierzęta na farmie[326].

Dlaczego pojawił się *pharming*? Otóż, popularność ataków typu *phishing* sprawiła, że użytkownicy stali się bardziej świadomi czyhającego na nich w sieci niebezpieczeństwa. Użytkownicy przestali reagować na otrzymywaną rzekomo z banku korespondencję elektroniczną, w której proszeni byli o ujawnienie swoich danych, zaczęli własnoręcznie wpisywać adres strony internetowej banku w pasku przeglądarki, zamiast korzystania z linków zamieszczonych w wiadomościach lub na stronach internetowych, sprawdzali certyfikat strony logowania przed każdorazowym wprowadzeniem danych – a więc, zaczęli przestrzegać sposoby uniknięcia większości dotychczas spotykanych zagrożeń. Łatwe do przeprowadzenia ataki, takie jak *phishing*, można równie łatwo wykryć. Wystarczy odpowiednia edukacja klientów, której banki starają się nie zaniedbywać. Cała ta sytuacja wręcz motywuje cyberprzestępców do obmyślania bardziej skomplikowanych metod wyłudzania poufnych danych. Jedną z nich jest właśnie *pharming*, nazywany też zatruwaniem pamięci DNS (ang. *DNS cache poisoning*).

2.3.2. Sposób działania sprawców *pharmingu*

Przestępcy najczęściej popełniając *pharming* manipulują „pytaniami o kierunek" zgłaszanymi przez komputer w celu odnalezienia żądanej strony internetowej, co w konsekwencji powoduje dyskretne przekierowanie użytkownika do fałszywej witryny stworzonej przez sprawcę. Skutek ten możliwy jest do osiągnięcia na dwa sposoby. Pierwszy sposób polega na ingerencji w pamięć podręczną DNS[327] komputera lokalnego, drugi na ingerencji w pamięć adresów DNS na serwerze[328].

---

[325] Seesee D., Weinhardt C., Schlottmann F. 2008: Handbook on Information Technology in Finance, Springer, Heidelberg, s. 737.

[326] Popp A. 2006: Phishing, pharming und das Strafrecht, „Multimedia und Recht" nr 2, s. 84.

[327] DNS (ang. Domain Name System, system nazw domenowych) – system serwerów, protokół komunikacyjny oraz usługa zapewniająca zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki wykorzystaniu DNS nazwa mnemoniczna, np. pl.wikipedia.org, może zostać zamieniona na odpowiadający jej adres IP, czyli 91.198.174.232. Usługa DNS warstwy aplikacji modelu TCP/IP, jest związana z portem 53 TCP/UDP. Źródło: http://pl.wikipedia.org/wiki/Domain_Name_System (dostęp 24.01.2012).

[328] Kiedrowicz-Wywiał A. 2011: Pharming i jego penalizacja, „Prokuratura i Prawo" nr 6, s. 24.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Ingerencja w pamięć podręczną DNS komputera lokalnego

W chwili, gdy użytkownik wpisuje w pasek przeglądarki internetowej adres witryny (np. www.nazwabanku.pl) i zatwierdza jej wybór, komputer dokonuje jego translacji na postać numerycznego adresu IP (np. XXX.XX.XX.XXX), który umożliwi odnalezienie tej konkretnej strony w sieci. Tłumaczenie następuje poprzez sprawdzenie adresu w tabelach, dostępnych w bazach danych 13 głównych serwerów DNS na świecie (tzw. *gold standard* DNS). Aby przyspieszyć ten proces, komputer zapisuje zazwyczaj kopie odpowiedzi dla odwiedzonych wcześniej stron w tzw. pamięci podręcznej DNS. Operacja ta sprawia, że nie jest konieczne każdorazowe wysyłanie zapytania do serwera. Jeśli jednak sprawcy uda się zmodyfikować treść pamięci, czyli zamiast adresu IP 195.72.35.111, wprowadzi adres podrobionej strony IP 506.89.32.255, to po wpisaniu przez użytkownika adresu www.nazwabanku.pl komputer za każdym razem skieruje użytkownika pod niewłaściwy adres, użytkownik zostanie przekierowany na stronę stworzoną przez cyberprzestępcę. Trzeba przy tym podkreślić, że wyświetlany w pasku przeglądarki adres będzie właściwy[329].

Aby przekierować użytkownika na sfałszowaną stronę logowania do konta bankowego, cyberprzestępcy nie muszą wysyłać mu żadnych wiadomości. Wystarczy, że zmienią adresy DNS na komputerze lub serwerze ofiary. Podstawowym zadaniem systemu nazw domenowych jest przekształcanie adresów stron znanych internautom na adresy zrozumiałe dla urządzeń tworzących sieć komputerową.

Modyfikacja pamięci podręcznej DNS (zwana inaczej „zatruwaniem" adresów DNS) jest możliwa dzięki wykorzystaniu konia trojańskiego. Są to dodatkowe instrukcje dopisane najczęściej do załączników wiadomości poczty elektronicznej lub bezpłatnego oprogramowania dostępnego w Internecie (takich jak gry, wygaszacze ekranu, programy pornograficzne). Po ich instalacji koń trojański zaczyna wykonywać pewne dodatkowe funkcje, umożliwiając hakerom np. zdalny dostęp do zainfekowanego komputera[330].

Ingerencja w pamięć adresów DNS na serwerze

Zdaniem A. Kiedrowicz - Wywiał, dzięki modyfikacji pamięci podręcznej DNS komputera lokalnego sprawca może dokonać przekierowania na spreparowaną przez siebie witrynę wyłącznie tych użytkowników, którzy z danego urządzenia korzystają. O wiele bardziej atrakcyjne może być

[329] Ibidem, s. 26.
[330] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

uzyskanie dostępu do pamięci podręcznej serwera używanego przez usługodawcę internetowego, gdyż również tam są przechowywane wzory najczęstszych translacji. W takiej sytuacji wszyscy użytkownicy korzystający z danego serwera są przekierowywani (mimo podania innego adresu) na stronę sprawcy, gdzie są następnie proszeni o zalogowanie się. Prócz ujawnienia istotnych danych identyfikacyjnych, może to również oznaczać pobranie do komputera koni trojańskich lub oprogramowania typu *spyware*, które będzie służyć do dalszej inwigilacji. Z uwagi na stosowane zabezpieczenia zatruwanie pamięci DNS serwerów jest stosunkowo trudne, i co za tym idzie, dość rzadkie. Coraz częściej natomiast notuje się tego typu ataki wobec użytkowników prywatnych[331].

Na uwagę zasługuje fakt, iż istnieje kilka sposobów zatruwania pamięci DNS. Najbardziej rozpowszechniony polega na zarażeniu systemu ofiary odpowiednim „koniem trojańskim". Nie brakuje wśród nich szkodników stworzonych w celu modyfikowania ustawień DNS na zainfekowanym komputerze użytkownika. W wyniku ich działania zmianie ulega mapowanie nazw domen do konkretnych adresów IP. Użytkownik, jak w zaprezentowanym wyżej przykładzie, po wpisaniu adresu swego banku może znaleźć się na stronie, która będzie wierną kopią oryginalnej witryny. Zalogowanie się na niej będzie skutkować kradzieżą realnych środków zgromadzonych na jego koncie[332].

Kolejną metodą, jest tzw. *drive-by pharming*, czyli zagnieżdżanie w kodzie tworzonych przez cyberprzestępców stron skryptów pisanych w języku JavaScript. Odnośniki do tych witryn są publikowane w serwisach społecznościowych, takich jak Facebook czy Twitter. Oszuści starają się też wypozycjonować je w wynikach wyszukiwania, używając w tym celu aktualnych, wzbudzających zainteresowanie tematów. Jeżeli internauta nabierze się i odwiedzi którąś z nich, zaimplementowany na stronie skrypt zmieni ustawienia DNS na jego routerze lub w punkcie dostępu bezprzewodowego. Może do tego dojść, jeśli router nie będzie chroniony hasłem albo hasło okaże się łatwe do odgadnięcia[333].

Najtrudniejszą do zatrucia jest pamięć podręczna na serwerze dostawcy Internetu. Również, tak jak komputery użytkowników indywidualnych, zapisuje on w niej żądania DNS. Jeżeli cyberprzestępcy uda się je sfałszować, to przez pewien czas (nieprzekraczający zwykle kilku godzin) użytkownicy,

[331] Ibidem, s. 26-27.
[332] Źródło: http://di.com.pl/porady/34094,0,Pharming_-_strategie_ataku_i_sposoby_obrony.html (dostęp 10.03.2015).
[333] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

którzy wpiszą w przeglądarce adres obranego za cel banku, zostaną przekierowani na podrobioną stronę. Umożliwi to pozyskanie dużej ilości poufnych danych za jednym zamachem. Na tego typu ataki narażeni są usługodawcy, którzy niesystematycznie aktualizują oprogramowanie zainstalowane na używanych urządzeniach[334].

Obojętnie, którą z opisanych wyżej metod zastosował haker, dalszy przebieg wydarzeń jest zawsze identyczny. Użytkownik, wprowadzając adres żądanej strony, przekonany jest, że znajduje się na stronie internetowej swojego banku. Na pasku adresu widzi bowiem ten sam adres co zwykle, a strona wygląda wręcz identycznie lub bardzo podobnie do tej, którą widzi przy każdorazowej próbie zalogowania się, nie podejrzewając żadnego zagrożenia, podaje cenne dla siebie (a przede wszystkim dla hakera) dane.

2.3.3. Wykrywanie i zwalczanie pharmingu

Niestety, nawet obeznany w zagadnieniach związanych z bezpieczeństwem informatycznym użytkownik może mieć poważny problem z wykryciem *pharmingu*. Tu bardzo duże pole do popisu mają administratorzy serwerów DNS, twórcy przeglądarek internetowych oraz zespoły zarządzające zagrożonymi witrynami. Trudności w wykryciu *pharmingu* wiążą się przede wszystkim z podejmowanymi działaniami, w wyniku których internauta zostaje przekierowany na stworzoną przez hakera stronę internetową. Ten może zachować się w dwojaki sposób: „zatruwa DNS" (jeśli chce dokonać ataku na skalę masową) lub modyfikuje plik znajdujący się na komputerze użytkownika, który ma stać się podmiotem kradzieży (wtedy atak jest ukierunkowany na osobę X, choć nie wyklucza to przypadkowości)[335].

Modyfikując pamięć DNS, sprawca niewątpliwie dokonuje zamachu na integralność danych informatycznych. Działanie takie wyczerpuje znamiona przestępstwa opisanego w art. 268 k.k. („§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią; § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych") i zagrożone jest karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do lat 2. Natomiast w przypadku, gdy czyn dotyczy zapisu na informatycznym nośniku danych, zagrożony jest

[334] Ibidem.
[335] Jeleśniański M.: op. cit.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

karą pozbawienia wolności do lat 3. Art. 268 k.k. określa przestępstwo udaremniania lub znacznego utrudniania dostępu do informacji osobie do tego uprawnionej. Penalizowane działanie polegać może na zniszczeniu (tj. całkowitym unicestwieniu), uszkodzeniu, usunięciu lub bezprawnej zmianie zapisu istotnej informacji, przy czym mamy tu na myśli ingerencję dotyczącą wszelkich urządzeń lub przedmiotów zawierających zapis informacji[336].

Czyn określony w art. 268 k.k. jest przestępstwem skutkowym, które zostaje dokonane w chwili, gdy sprawca udaremnił lub znacznie utrudnił osobie uprawnionej zapoznanie się z zapisem istotnej informacji. Głównym przedmiotem ochrony tej regulacji jest, co podkreśla Adamski, dostępność informacji[337]. Podstawowym celem działania sprawcy *pharmingu* nie jest jednak utrudnianie dostępu do informacji, gdyż takie działanie mogłoby jedynie zaalarmować użytkownika i sprawić, że atak zakończyłby się niepowodzeniem, tym niemniej konsekwencją zmiany pamięci DNS jest niewątpliwie utrudnienie dostępu do zapisu informacji, jakim jest właściwy adres witryny. Trudności tych doświadcza jednak nie użytkownik, lecz komputer. Znamię znacznego utrudnienia osobie uprawnionej zapoznania się z zapisem informacji nie zostanie wręcz spełnione. Co więcej, utrudnienia tego nie sposób uznać za znaczne, skoro odtworzenie zmodyfikowanego zapisu jest w prosty sposób możliwe, gdyż jego kopie znajdują się na serwerach[338]. Zatem znamiona określone w art. 268 § 2 k.k. nie obejmują swoim zakresem ataków typu *pharming*.

Konwencja Rady Europy dotycząca ścigania cyberprzestępstw, którą Polska podpisała w 2001 roku wprowadziła powinność objęcia zakresem regulacji karnej działań polegających na umyślnym uszkadzaniu, usuwaniu, niszczeniu, zmienianiu lub blokowaniu danych informatycznych bez uprawnienia. Przepisy te chronić miałyby zarówno dane, jak i programy komputerowe przed zamachami na ich integralność i być odpowiednikiem norm karnych zakazujących niszczenia lub uszkadzania rzeczy[339]. W wyniku tego wymogu uchwalona została ustawa z dnia 18 marca 2004 roku o zmianie ustawy kodeksu karnego, ustawy kodeks postępowania karnego oraz ustawy kodeksu wykroczeń[340], która wprowadziła do kodeksu karnego art. 268a, mający czynić zadość wymaganiom zawartym w Konwencji. Według przepisów przedmiotowego artykułu każdy, „kto nie będąc do tego uprawnionym,

[336] Marek A.: op. cit., s. 669.
[337] Adamski A.: Prawo karne…, op. cit., s. 66.
[338] Ibidem, s. 72.
[339] Adamski A. 2001: Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, Dom Organizatora, Toruń, s. 28.
[340] Dz. U. Nr 69, poz. 626.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlegał karze pozbawienia wolności do lat 3". Postać, jaką nadano treści tego przepisu sprawia, że przedmiotem jego ochrony jest dostępność danych informatycznych, a nie ich integralność. Jednym ze znamion art. 268a k.k. jest natomiast zakłócenie automatycznego przetwarzania danych informatycznych. Wydaje się, że modyfikowanie pamięci DNS wyczerpuje znamiona tego przepisu; proces przetwarzania danych nie zostaje zatrzymany, lecz przebiega w sposób odmienny od zamierzonego, a więc jest zakłócony[341].

Podobnie sprawa przedstawia się w przypadku art. 269a k.k. („Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej"), który penalizuje zmianę danych informatycznych w istotnym stopniu zakłócających pracę systemu komputerowego lub sieci teleinformatycznej. Nie sposób się przy tym zgodzić z argumentacją, iż ustawodawca uzależnił odpowiedzialność od istotności zmodyfikowanych przez sprawcę danych. Znamię to, zarówno w art. 268a k.k., jak też art. 269a k.k., odnosi się bowiem do stopnia zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej. Mimo, że w przypadku ataków typu *pharming* konsekwencje tego typu modyfikacji mogą być istotne, wątpliwym jest, czy sama modyfikacji pamięci DNS komputera domowego spowoduje istotne zakłócenie pracy systemu. Bardziej zasadne byłoby takie stwierdzenie w sytuacji zmiany danych umieszczonych na serwerze (ze względu na większy zasięg zakłócenia), co – jak już wspomniano – jest sytuacją zdecydowanie rzadszą[342].

Zdaniem Adamskiego w literaturze niejednokrotnie akcentowany był problem krzyżowania się zakresów karalności art. 268a k.k. i art. 269a k.k.[343] Trudno przy tym wyłączyć stosowanie któregoś z tych przepisów w oparciu o zasadę *lex specialis*, czy też *lex consumens*. Zdaje się więc, że czyn sprawcy należałoby zakwalifikować na podstawie obu zbiegających się przepisów, sąd natomiast winien wymierzyć karę na podstawie art. 269a k.k., jako zawierającego wyższą sankcję karną (zgodnie z art. 11 § 2 k.k.). Sytuacja ta, zdaniem Kiedrowicz-Wywiał, świadczy jednak o braku konsekwencji ustawodawcy[344].

[341] Kiedrowicz-Wywiał A.: op. cit., s. 29.
[342] Ibidem.
[343] Adamski A.: Cyberprzestępczość – aspekty prawne i kryminologiczne, Studia Prawnicze nr 4/2005, s. 58.
[344] Kiedrowicz-Wywiał A.: op. cit., s. 30.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Zaakcentować należy, iż modyfikacja pamięci DNS oraz spreparowanie witryny internetowej jest zaledwie środkiem do celu sprawcy, jakim w konsekwencji jest uzyskanie danych uwierzytelniających niezbędnych do przejęcia środków zgromadzonych na koncie użytkownika. Sprawca jest motywowany chęcią zdobycia korzyści majątkowej. Jednakże zakwalifikowanie tego typu czynu jako oszustwa z art. 286 k.k. albo oszustwa komputerowego z art. 287 k.k., może budzić pewne wątpliwości. W konstrukcji przestępstwa z art. 286 k.k. sprawca oddziałuje na proces decyzyjny osoby przez niego oszukiwanej. Może być to zarówno osoba fizyczna występująca we własnym imieniu, jak też reprezentująca osobę prawną lub też jednostkę organizacyjną nieposiadającą osobowości prawnej[345]. Inaczej natomiast sprawa wygląda w przypadku oszustwa komputerowego. Tutaj nie występuje element wprowadzenia innej osoby w błąd, bądź też wykorzystania tego błędu[346], ponieważ bezpośrednim przedmiotem oddziaływania sprawcy nie jest inna osoba, lecz urządzenie bądź system komputerowy[347]. Brak elementu oddziaływania sprawcy na proces decyzyjny poszkodowanego uważa się wręcz za element konstytutywny znamion przestępstwa oszustwa komputerowego[348]. W przypadku *pharmingu*, w pierwszej fazie ataku (manipulacja pamięcią DNS), przedmiotem oddziaływania sprawcy jest niewątpliwie system komputerowy. Niemniej jednak w momencie, gdy użytkownik zostanie odesłany do fałszywej witryny internetowej, można mówić o oddziaływaniu na jego proces decyzyjny. Sprawca bowiem, uzyskując nieprzeznaczone dla niego dane, wykorzystuje fakt, iż witryna ta nie jest oryginalną stroną logowania banku. Zdaniem Kiedrowicz-Wywiał[349], już samo dokonanie modyfikacji w pamięci DNS z zamiarem osiągnięcia w późniejszym okresie korzyści majątkowej stanowić będzie przestępstwo oszustwa komputerowego. Podkreślić przy tym należy, że atak typu *pharming*, nawet na etapie uzyskania już przez sprawcę korzyści majątkowej, nie będzie stanowił przestępstwa oszustwa określonego w art. 286 k.k. Do jego bytu niezbędna jest bowiem tożsamość osoby wprowadzonej w błąd oraz rozporządzającej mieniem[350]. W sytuacji, gdy sprawca uzyskuje korzyść majątkową w wyniku samodzielnego działania (np. poprzez dokonanie przelewu z cudzego konta, dzięki zdobytym wcześniej danym uwierzytelniającym), nie

[345] Ibidem, s. 31.
[346] Adamski A.: Prawo…, op. cit., s. 115.
[347] Korczyński R., Koszut R. 2002: Oszustwo komputerowe, „Prokuratura i Prawo" nr 2, s. 20.
[348] Kardas P. 2000: Oszustwo komputerowe w kodeksie karnym, „Przegląd Sądowy" nr 11-12, s. 52.
[349] Kiedrowicz-Wywiał A.: op. cit., s. 32.
[350] Zob. postanowienie SN z dnia 29 stycznia 2004 r., sygn. I KZP 37/03, „Prokuratura i Prawo" nr 3/2004, dodatek „Orzecznictwo".

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

zostaje wypełnione znamię „doprowadzenia do niekorzystnego rozporządzenia mieniem”[351].

Niewątpliwie oszustwo komputerowe jest przestępstwem kierunkowym. Pociągnięcie sprawcy do odpowiedzialności będzie wymagało wykazania, iż działał on w celu osiągnięcia korzyści majątkowej lub też wyrządzenia innej osobie szkody. W takiej sytuacji, na zasadzie *lex consumens,* wyłączony zostanie zbieg art. 268a k.k. lub art. 269a k.k. z art. 287 k.k.[352]

Działanie sprawcy *pharmingu* w przypadku ataków na klientów bankowości internetowej, polega na ingerencji w dane informatyczne, a celem tego działania jest oczywiście osiągnięcie korzyści majątkowej – tym samym będzie ono penalizowane na gruncie art. 287 k.k. (oszustwo komputerowe). Pewne wątpliwości, zdaniem Kiedrowicz-Wywiał budzić może zakwalifikowanie modyfikacji pamięci DNS, jako przestępstwa z art. 268a k.k. i 269a k.k. z uwagi na występujące w tych przepisach znamię istotności stopnia zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej. Sankcji prawno-karnych nie przewidziano jedynie za umieszczenie w Internecie spreparowanej witryny internetowej – osoby poszkodowane takim działaniem (tj. instytucje finansowe) muszą szukać ochrony na gruncie prawa cywilnego[353].

2.4. Przestępcze wykorzystanie numerów kart płatniczych – *carding*

Wraz z rozwojem Internetu stopniowo upowszechniał się także handel dokonywany za jego pośrednictwem (tzw. handel online). W przypadku handlu on-line płatności dokonywano najczęściej kartami kredytowymi, co przy jednoczesnym braku uniwersalnej i skutecznej metody ochrony danych w trakcie ich przesyłania z przeglądarki internetowej do serwera, sprawiło, że rozwinęła się w Internecie sztuka oszukiwania związana z kartami kredytowymi i telefonicznymi. Proceder ten polega generalnie na zdobywaniu prawdziwych danych – numerów istniejących kart płatniczych, bądź – tworzeniu fałszywych. Powstały nawet specjalne programy, które umożliwiają generowanie fałszywych numerów kart, w oparciu o różne formuły charakterystycznych dla poszczególnych organizacji kart płatniczych (Visa International, MasterCard, czy American Express).

[351] Kiedrowicz-Wywiał A.: op. cit., s. 32.
[352] Ibidem.
[353] Ibidem, s. 35.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Przestępstwo, o którym mowa to tzw. *carding*. Jest to przestępstwo polegające na nielegalnym wykorzystaniu numerów kart płatniczych. W przypadku *cardingu* przedmiotem wykonawczym nie jest karta płatnicza, a jedynie jej numer. Numer karty płatniczej, a nie dane dotyczące jej posiadacza, czy też termin ważności, jest dla *cardera* (sprawcy dokonującego przestępstwa *cardingu*) najistotniejszą informacją. Numery kart płatniczych są wręcz na wagę złota. Głośny był przypadek Carlosa Felipe Salgado, który włamał się do komputera jednego z *providerów* w San Diego kradnąc numery ponad 100 000 kart kredytowych z zamiarem ich sprzedaży on-line. Straty spowodowane przez *carding* w samych tylko Stanach Zjednoczonych oceniane są na około miliard dolarów rocznie[354].

Carding polega na posługiwaniu się bez upoważnienia danymi z karty płatniczej przy dokonywaniu zamówień pocztowych, telefonicznych lub za pomocą sieci komputerowej. Z uwagi na znaczne przywiązanie klientów do tradycyjnych form dokonywania transakcji handlowych przestępstwo *cardingu* jest w Polsce mało popularne, a tego typu działania sprawców występują stosunkowo rzadko[355], choć ostatnio coraz częściej można usłyszeć o aresztowaniach młodych ludzi za korzystanie z cudzych kont bankowych. Wśród samych *carderów* panuje powszechne przekonanie, że Polacy nie mają pojęcia o *cardingu*, natomiast w Niemczech jest to już spory problem[356].

Pozyskiwanie cudzych numerów kart płatniczych może nastąpić na kilka sposobów. Opiera się ono głównie na 4 metodach:

1) metodzie „mechanicznej" (lub elektronicznej) – sprawcy pozyskują tutaj numer kart płatniczych za pomocą technik komputerowych – programów szpiegowskich typu *spyware*, koni trojańskich, wirusów oraz za pomocą tzw. *pharmingu* (czyli nieświadomego korzystania przez ofiarę z „podrobionej" strony internetowej np. fałszywej strony banku);
2) metodzie wyłudzenia danych (nazywana z angielskiego *scam*) – sprawcy poprzez różnego rodzaju pozorne działania (np. rzekomy telefon z banku lub e-mail od banku z prośba o odpowiedź) wyłudzają dane dotyczące kart płatniczych bezpośrednio od ofiary;

[354] Miejskie zagrożenia – Carding, http://www.inkluz.pl/archiwum/inkluz62/main/vr.html (dostęp 01.09.2013).
[355] Niedźwiecka-Małecka M.: op. cit., s. 177.
[356] Zob. Bothunters.pl, Polacy nie mają pojęcia o Hardingu – część II wywiadu z carderem, Dziennik Internautów z 10.11.2010, http://di.com.pl (dostęp 01.09.2013).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

3) metodzie „podejrzenia" danych – sprawcy pozyskują te dane wskutek obserwacji danej osoby lub grupy osób w różnych sytuacjach (np. podglądają lub fotografują numer karty kredytowej);
4) metodzie zakupu danych od nieuczciwych osób mających dostęp do baz danych banków oraz innych instytucji przetwarzających takie dane[357].

Można tu jeszcze wspomnieć o innych metodach zdobywania numerów kart płatniczych, jak chociażby tzw. *trash diving,* czyli metodzie polegającej na przeszukiwaniu zawartości kosza na śmieci, gdzie wyrzucane są paragony z numerami kart ze sklepów i placówek, w których dokonano płatności za pośrednictwem karty kredytowej, czy chociażby tzw. generator – wykorzystanie ściągniętych z Internetu programów, które generują numery kart kredytowych (np. Credit Master czy Credit Wizard). Istnieje również metoda uzyskiwania numeru karty kredytowej na telefon, która polega na prowadzeniu przez *cardera* rozmowy telefonicznej z posiadaczem karty kredytowej. W przypadku tej metody istotne jest to, aby *carder* wiedział, w którym banku jego ofiara posiada rachunek. Przykładów przeprowadzania tego typu rozmów nie brakuje na zakonspirowanych forach internetowych użytkowanych przez *carderów*. Jak może przebiegać tego typu rozmowa, przedstawiono poniżej:

- OSZUST: Dzień dobry, Czy rozmawiam z panem Piotrem Janowskim ?
- KLIENT: Tak to ja.
- O: Moje nazwisko Halina Dzięcioł. Dzwonie z Banku PKO BP SA w sprawie pana konta.
- K: Tak?! A co się stało?
- O: Limit pana karty został zmniejszony do 500 zł.
- K: Ależ to niemożliwe! Mój limit wynosi 10 tys. zł.
- O: Hmm. Być może zaszła jakaś pomyłka w komputerze. Czy mogę prosić o podanie numeru karty oraz datę ważności w celu weryfikacji?
- K: Tak, oczywiście. Numer to XXXX-XXXX-XXXX-XXXX, a termin ważności to XX/XX.
- O: Dziękuję, postaramy się sprawę szybko wyjaśnić. Do usłyszenia.
- K: Do widzenia[358].

[357] Szymczykiewicz R. 2011: Czym jest carding? Artykuł z dnia 20.12., http://prawo-karne.wieszjak.pl/przestepstwa-komputerowe/298323,2,Czym-jest-carding.html (dostęp 10.03.2015).
[358] Zob. Żwiruk K. 2004: Carding – przestępcze wykorzystanie numerów kart płatniczych, 19.05. http://kartyonline.pl/arty.php?id=99 (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Na takich zakonspirowanych forach przestępcy, których działania nie są przez nikogo zakłócane spokojnie negocjują oferty zakupu i sprzedaży skradzionych danych kart.

Proceder *cardingu* przebiega w następujący sposób:

1. Oszust przesyła skradzione informacje o kartach płatniczych swojemu koledze, tak zwanemu *carderowi* i informuje go, jakie towary ma zakupić i do kogo je przysłać.
2. *Carder* opracowuje spis sklepów internetowych z niewystarczającymi zabezpieczeniami i zamawia w nich wybrane towary, wykorzystując do płatności skradzione dane kart kredytowych. Jako odbiorcę towarów podaje jednego lub kilku pośredników.
3. Pośrednicy odbierają towary osobiście lub w punktach odbioru paczek, a następnie przekazują je oszustowi, który towary zachowuje dla siebie lub sprzedaje je na aukcjach internetowych, dzieląc się zyskami z *carderem*.

Oszuści przekazują *carderowi* skradzione numery kart kredytowych, które ten wykorzystuje do zamawiania jak najdroższych artykułów w sklepach internetowych. Odbiorcą jest z reguły niczego niepodejrzewający pośrednik, który osobiście odbiera towary w punkcie odbioru paczek i przekazuje je przestępcom.

Pośrednicy są najczęściej werbowani za pomocą drobnych ogłoszeń lub tzw. spamu. Mając nadzieję na kilkadziesiąt złotych dodatkowego dochodu, często nie przeczuwają nawet, że odgrywają rolę pasera na zlecenie cyberprzestępców. Ponieważ pierwsi mają kontakt z towarem, są też pierwszym adresem, pod który puka Policja, bo w międzyczasie właściciel karty zauważył podejrzane obciążenie i wstrzymał płatność. Poza właścicielem karty do listy przegranych w tej perfidnej grze dołącza także pośrednik i sklep internetowy realizujący zamówienie[359].

Rzadko się zdarza, że w przestępstwie *cardingu* bierze udział pojedyncza osoba, zazwyczaj jest to grupa licząca od kilku do kilkunastu osób: zleceniodawców, pośredników i informatorów. Zadania takiej grupy rozciągają się od wyszukiwania sklepów internetowych ze słabymi zabezpieczeniami, przez tworzenie szkodliwego oprogramowania, aż po handel skradzionymi danymi. Kontakty i wspólne przedsięwzięcia planowane są za pośrednictwem zakonspirowanych forów internetowych. Handel skradzionymi danymi kart kredytowych stanowi dla nich wprawdzie niewielką, ale wciąż rosnąca liczba

[359] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

postów. Na tych forach można się zarejestrować dopiero po rekomendacji ze strony innego członka grupy[360]. Z reguły grupy trudniące się *cardingiem* są dobrze zorganizowane i wyspecjalizowane. Część osób w takiej grupie zajmuje się pozyskiwaniem numerów kart, co następuje poprzez Internet lub też z zastosowaniem innych metod. Inni członkowie grupy zajmują się dokonywaniem transakcji, inni zaś odbiorem towarów i ich późniejszą odsprzedażą. Tego rodzaju grupy są trudniejsze do wyśledzenia, działając w Internecie starają się one nie pozostawiać po swoich działaniach żadnych śladów[361].

Jak zatem można chronić się przed przestępstwem *cardingu?* Przede wszystkim należy chronić numer posiadanej karty kredytowej i ostrożnie obchodzić się z kartą, co powinno stać się żelazną zasadą. Niestety, dotychczas nie zostały wdrożone na pełną skalę technologie oparte o 3D Secure, takie jak chociażby Verified by Visa, które wymagają, aby do zakupu w Internecie był niezbędny nie tylko numer karty, ale także dodatkowe hasło. Posiadacz karty ustala w hasło banku , który wydał jego kartę. System ten zapewnia nieporównywalnie większe bezpieczeństwo zakupów od obowiązującego obecnie rozwiązania[362]. Warto również przestrzegać następujących zasad:

1. Uważajmy na adres: dokonując w Internecie płatności kartą, sprawdźmy, czy adres strony internetowej rozpoczyna się od https://, a nie od http://. Połączenia szyfrowane są generalnie bezpieczniejsze dla użytkownika.
2. Sprawdzajmy certyfikaty: podczas dokonywania płatności kliknijmy na symbol kłódki w polu adresu i sprawdźmy, czy certyfikat bezpieczeństwa wystawiony jest na firmę, która obsługuje płatność.
3. Test na początek: dokonując pierwszego zakupu w nowym sklepie internetowym, o ile to możliwe, powinniśmy najpierw dokonać zakupów na niewielką sumę.
4. Zwiad: dokonując zakupów w nieznanym dotychczas sklepie, zasięgnijmy informacji na temat sprzedającego – często wystarczy tylko wpisać jego nazwę do wyszukiwarki. W ten sposób dowiemy się, czy inni klienci nie mieli już z danym sprzedawcą przykrych doświadczeń.
5. Kontrola: sprawdzajmy na wyciągu z karty, czy nie ma na nim podejrzanych pozycji[363].

[360] Ibidem.
[361] Ibidem.
[362] Ibidem.
[363] Źródło: http://www.komputerswiat.pl/jak-to-dziala/2010/06/carding-jak-dzialaja-zlodzieje-kart-kredytowych,4.aspx# content – 29.06.2010 (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Odpowiadając na pytanie, jak nie paść ofiarą *cardingu*, należy powtórzyć w istocie wszystkie zalecenia związane z tym, jak nie paść również ofiarą kradzieży tożsamości. Zatem należy: zabezpieczać komputer stosownymi programami antywirusowymi; nie podawać pochopnie danych osobowych w Internecie oraz osobom trzecim; strzec się podawania danych w dziwnych sytuacjach (np. nr PESEL telemarketerowi), a także pilnować dokumentów osobistych oraz kart płatniczych i niezwłocznie zgłaszać zagubienie lub kradzież dokumentów lub kart płatniczych na policję, do banków, itd.[364].

Przestępstwo *cardingu* kwalifikowane jest w polskim ustawodawstwie karnym, jako czyn z art. 286 § 1 k.k. § 1. („Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania"), czyli oszustwo zwykłe, zagrożone karą pozbawienia wolności od 6 miesięcy do lat 8. Sprawca, co podkreśla Niedźwiedzka-Małecka, posługuje się autentycznymi numerami cudzych kart w celu uzyskania towaru lub usługi. Tym samym jego działanie jest podjęte w celu osiągnięcia korzyści majątkowej, a czynności sprawcze polegają np. na wprowadzeniu w błąd osoby przyjmującej zamówienie. W wyniku tak opisanych działań, inna osoba dokonuje niekorzystnego rozporządzenia mieniem własnym lub cudzym[365].

Z kolei Adamski stoi na stanowisku, iż w przypadku przestępstwa *cardingu* zastosowanie powinna znaleźć nie tylko kwalifikacja z art. 286 § 1 k.k., czyli oszustwo zwykłe, ale także kwalifikacja z art. 287 § 1 k.k. – oszustwo komputerowe[366]. W ocenie Niedźwieckiej-Małeckiej, trudno zgodzić się z twierdzeniem Adamskiego, co do tego, że zamówienie za pośrednictwem telefonu towarów lub usług wyczerpuje znamiona określone w art. 287 § 1 k.k. Linia telefoniczna nie jest bowiem nośnikiem zawierającym, przetwarzającym, gromadzącym lub przesyłającym informacje, do którego odnosi się art. 287 § 1 k.k. O kumulatywnej kwalifikacji może być zaś mowa w przypadku wykorzystania przez sprawcę sieci komputerowej, np. internetowej. Jest to możliwe bowiem w art. 287 k.k. jest mowa o wpływaniu na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub o zmianie, usuwaniu albo wprowadzaniu nowych zapisów na komputerowym nośniku informacji, które to działania powinny zostać dokonane na nośniku zawierającym, przetwarzającym, gromadzącym lub przesyłającym informacje[367].

[364] Szymczykiewicz R.: Czym jest carding…, op. cit.
[365] Niedźwiecka-Małecka M.: op. cit., s. 178.
[366] Adamski A.: Prawo …, op. cit., s. 97.
[367] Niedźwiecka-Małecka M.: op. cit., s. 178.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

2.5. Inne przestępstwa w bankowości internetowej

2.5.1. Kradzież haseł, kodów jednorazowych i narzędzi

W przypadku kradzieży haseł, kodów jednorazowych i narzędzi (np. token, telefon komórkowy), które służą do autoryzacji dostępu do rachunku i dokonywania transakcji internetowych, przestępcy wykorzystują fakt zapisywania przez klientów banku tego typu danych w jawnej formie, czy to w postaci odręcznej notatki, czy też notatki zapisywanej w pamięci telefonu komórkowego lub podobnego urządzenia. Kradzież taka może zostać dokonana bezpośrednio lub zdalnie.

Jak podkreśla Szwajkowska i inni autorzy[368], aby ustrzec się przed przestępstwem bezpośredniej kradzieży danych autoryzacyjnych, pamiętać należy, aby tego typu dane nie były zapisywane w jawnej formie i żeby były przechowywane w bezpiecznym miejscu. Każdy przypadek utraty narzędzi służących do autoryzacji transakcji dokonywanych w bankowości internetowej powinien być niezwłocznie zgłaszany do banku. Jeżeli utracony został telefon komórkowy, który wykorzystywany był do dokonywania transakcji w bankowości internetowej, należy w pierwszej kolejności zablokować dostęp do rachunku bankowego (poprzez Internet), a następnie dezaktywować utraconą kartę SIM. Nie należy także w pamięci telefonu komórkowego zapisywać loginów i kodów dostępu do rachunków bankowych wykorzystywanych w bankowości internetowej.

Przestępstwo zdalnej kradzieży haseł dostępu i kodów jednorazowych możliwe jest wyłącznie w przypadku ich zapisania na dysku komputera osobistego. Działanie sprawców w tym wypadku polega na wykorzystaniu specjalnego (złośliwego) oprogramowania lub luk w systemie zabezpieczeń komputera. Sposób działania sprawców szczegółowo opisany został w części przedmiotowego rozdziału dotyczącej włamań do komputerowych systemów informatycznych. W tym miejscu przedstawiony zostanie jedynie sposób zabezpieczenia się przed tego typu przestępstwami. Aby zabezpieczyć się przed zdalną kradzieżą danych wykorzystywanych do autoryzacji transakcji w bankowości internetowej, należy przestrzegać następujących zasad[369]:

[368] Szwajkowska G. i in.: op. cit., s. 33.
[369] Ibidem, s. 34-35.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

1) nie zapisywać na dysku twardym komputera informacji, które służą do autoryzacji transakcji w bankowości internetowej,
2) skonfigurować przeglądarkę internetową zgodnie z zaleceniami banku (tego typu zalecenia zamieszczane są na stronach internetowych banku),
3) korzystać z systemu haseł jednorazowych generowanych przez token lub otrzymywanych z banku za pośrednictwem wiadomości SMS,
4) właściwie skonfigurować stację roboczą (wyłączyć zbędne usługi i procesy, stosować hasła użytkownika komputera, szyfrować partycje komputera lub wrażliwe dane),
5) zainstalować oprogramowanie antywirusowe z licencjonowanego źródła (najlepiej typu Internet Security), właściwie je skonfigurować i na bieżąco aktualizować,
6) zainstalować oprogramowanie kontrolujące ruch sieciowy tzw. *firewall*, właściwie jej skonfigurować i na bieżąco aktualizować (oprogramowanie tego typu mają już programy typu internet security).

2.5.2. Sniffing (podsłuch)

Do grona przestępstw internetowych dokonywanych w bankowości elektronicznej zaliczyć należy także tzw. *sniffing*, o którym już wcześniej wspominano. Nazwa pochodzi od angielskiego słowa *sniff*, które oznacza wąchanie, obwąchiwanie[370]. Powszechnie mianem *sniffing* określa się węszenie. Technika ta początkowo została stworzona głównie na potrzeby administratorów i polegała na podsłuchiwaniu wszystkich pakietów, które krążyły po sieci komputerowej. Wykorzystywana była do dokonania analizy tych pakietów w celu wychwycenia jakichkolwiek nieprawidłowości w funkcjonowaniu sieci. Dzięki monitorowaniu pracy sieci administrator widział jej słabe i mocne punkty. Nie ulega wątpliwości, że s*niffing,* jako narzędzie administracyjne stwarza ogromne możliwości diagnostyczne. Jednakże w krótkim czasie zalety *sniffingu* zostały zauważone przez hakerów. Do analizy śledzonych pakietów stworzyli oni własne oprogramowanie, które

[370] Fisiak J., Adamska-Sałaciak A. i in. 2006: Longman. Słownik współczesny angielsko-polski, polsko-angielski, Bergamo, s. 408.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

umożliwia wychwycenie ważnych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe[371].

Przestępstwo *sniffingu*, pozwala osobom postronnym na uzyskanie danych przesyłanych przez sieć, ale nie wpływa na ich zawartość. Informacja niezmieniona i kompletna dociera do odbiorcy. Metoda ta ma, jak zatem widać, bierny charakter, nie stanowi w sposób bezpośredni większego zagrożenia. Jest jedynie narzędziem, które pozwala *snifferowi* na uzyskanie niezbędnych danych do realizacji innych przestępstw, bardziej niebezpiecznych i stanowiących bezpośrednie zagrożenie – przykładowo numer karty kredytowej zdobyty poprzez podsłuch sieci może zostać następnie wykorzystany przez osoby nieuprawnione do realizacji płatności[372].

Sprawca *sniffingu* swoim zachowaniem wyczerpuje znamiona czynu określonego w art. 267 § 3 k.k. („Kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowanie"), zagrożonego karą grzywny, karą ograniczenia wolności albo karą pozbawienia wolności do lat 2. Podkreślić należ, iż przepis art. 267 § 3 k.k. posiada cytowane brzmienie wprowadzone nowelizacją z dnia 24 października 2008 roku. Omawiany przepis stanowi, iż odpowiedzialności karnej podlega ten, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Oczywistym jest, że pomimo tego, iż sam program komputerowy nie jest urządzeniem, to już komputer z zainstalowanym właściwym programem (np. typu *password sniffer*) pozwalającym na monitorowanie ruchu w sieci i przechwytywanie początkowych sekwencji bajtów danej sesji zawierającej identyfikatory i hasła dostępu, będzie urządzeniem o charakterze specjalnym[373].

Przestępstwo z art. 267 § 3 k.k. jest przestępstwem umyślnym, które można popełnić tylko w zamiarze bezpośrednim, zaś osoba, która instaluje urządzenie podsłuchowe, np. na cudze zlecenie, ponosi odpowiedzialność karną na podstawie art. 267 § 3 k.k. tylko wówczas, jeżeli ma ona świadomość, iż nie jest uprawniona do zakładania tego rodzaju urządzeń. Osoba zlecająca takiego rodzaju działania odpowiadać będzie natomiast za sprawstwo kierownicze w zakresie polecenia popełnienia czynu z art. 267 § 3 k.k.[374]

---

371 Źródło: http://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=8 (dostęp 10.03.2015).

372 Zob. http://bankowoscinternetowa.republika.pl/html/Bezp.html (dostęp 11.03.2015).

373 Adamski A. 1998: Karalność hackingu na podstawie przepisów kodeksu karnego z 1997 r. „Przegląd Sądowy" nr 11-12, s. 156.

374 Adamski A.: Prawo…, op. cit., s. 64.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

2.5.3. Tampering

Kolejnym przestępstwem popełnianym w bankowości internetowej jest tzw. *tampering* (z ang. penetracja, manipulacja), który polega na przechwyceniu danych oraz ich modyfikacji przez osoby postronne. W konsekwencji do odbiorcy docierają informacje o zmienionej treści. Metoda ta stanowi bezpośrednie zagrożenie. W najlepszym wypadku może ona doprowadzić jedynie do nieporozumień. Jej skutki mogą być jednak znacznie poważniejsze. Włamywacze mogą zmienić parametry zlecenia przelewu klienta wprowadzając numer własnego rachunku, na który wpłyną pieniądze. W rezultacie naraża to na straty finansowe bank i klienta[375].

2.5.4. Spoofing

Spoofing – technika ataku IP (Internet Protocol) to jedna ze skuteczniejszych i częściej stosowanych metod nieautoryzowanego pozyskiwania informacji. Polega ona na „podszywaniu" się pod inny komputer w sieci. Haker, wysyłając pakiety z fałszywym adresem źródłowym, oszukuje komputer-odbiorcę, który błędnie identyfikując nadawcę, a wszystkie pakiety wysyła bezpośrednio do agresora. W ten sposób komputer hakera może udawać np. serwer, dzięki czemu może uzyskać dostęp do wszystkich tajnych danych. Powstało już mnóstwo wersji oprogramowania służącego to tego typu działań. Można je instalować zarówno na komputerze-agresorze, jak i samych urządzeniach dostępowych np. routerach. Taki atak na router może być bardzo groźny w skutkach, ze względu na to, że cały ruch w nim generowany może być kontrolowany przez hakera[376].

Spoofing jest metodą popełniania przestępstw w bankowości internetowej polegającą na podszywaniu się przez oszustów pod inną tożsamość, np. pod tożsamość banku. Metoda ta sprowadza się do ataku na system komputerowy, którego zadaniem jest zapewnienie bezpieczeństwa w sieci poprzez blokadę dostępu do tego systemu nieuprawnionych pakietów danych – tych, które nie dysponują określonym i zgodnym adresem IP oraz polega na przerobieniu przez hakera adresów IP na przesyłanych przez niego do systemu pakietach danych za pomocą posiadanego specjalnego oprogramowania, w taki sposób, by system rozpoznał te dane jako pochodzące z własnej sieci

[375] Źródło: http://bankowoscinternetowa.republika.pl/html/Bezp.html (dostęp 10.03.2015).
[376] Źródło: http://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=8 (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

informatycznej. W wyniku tego system, mylnie rozpoznawszy pakiety danych jako własne, nie dokonuje procedury sprawdzenia użytkownika, a w szczególności nie zadaje mu pytania o hasło dostępu uznając, iż uprzednio był już zalogowany w tym systemie. Jest to swoiste obejście zabezpieczeń przez hakera, który tym samym w ogóle nie musi uzyskać informacji o treści hasła dostępowego. Haker nie dokonuje więc przełamania zabezpieczeń elektronicznych, magnetycznych czy też innych, co powodowało, iż w sytuacji, gdy dodatkowo nie zapoznawał się z nieprzeznaczonymi dla niego informacjami – np. ściągając je w formie cyfrowej, zapisując na płytę CD-R i przekazując takie dane osobie zlecającej[377].

Sposób popełnienia przestępstwa *spoofingu* w bankowości internetowej można podzielić na dwie fazy – pierwsza polega na udawaniu banku przez przestępców. Podobnie, jak w przypadku *sniffingu,* etap ten służy głównie do uzyskania danych potencjalnych ofiar takich, jak imię, nazwisko, numer karty kredytowej, a przede wszystkim do zdobycia tajnego identyfikatora i hasła, które klienci wykorzystują podczas logowania się do systemu bankowości internetowej z portalu transakcyjnego banku. Sprawcy w tym wypadku wykorzystują nieuwagę klientów oraz błędy programowe przeglądarek internetowych. Przykładowo, w roku 2004 zdarzały się w Polsce próby tego typu oszustw. Beneficjenci banków PKO BP S.A oraz Citibank Handlowy posiadający konta internetowe w tych instytucjach otrzymywali pocztę elektroniczną rzekomo pochodzącą od banku. W rzeczywistości były to listy wysyłane przez przestępców, ale do złudzenia przypominające te, które klienci otrzymywali wcześniej od banku. Informowały one, że otwarty został nowy serwis transakcyjny i w celu jego sprawdzenia klienci proszeni są o jak najszybsze zalogowanie się do niego. W liście podawany był odnośnik do strony internetowej, na której można było to uczynić. Nie był to oczywiście nowy portal banku. Takiego w ogóle nie było. Serwis, na który trafiały osoby wykonujące instrukcje z otrzymanego e-maila, był w rzeczywistości fikcyjny, zbudowany przez oszustów i umieszczony na innym serwerze. Do złudzenia przypominał on prawdziwy portal banku. Na pasku adresowym przeglądarki widniał jego rzeczywisty adres. Zatem nie wzbudzało to żadnych podejrzeń wśród klientów, którzy bez większych obaw wpisywali swój identyfikator i hasło w celu zalogowania się, co oczywiście kończyło się niepowodzeniem. Jednocześnie dane umożliwiające dostęp do internetowego konta beneficjenta trafiały w ręce oszustów. Wtedy rozpoczynał się drugi etap *spoofingu,* gdy przestępcy wykorzystywali nielegalnie zdobyty login i hasło.

[377] Siemkowicz P.: op. cit, s. 7.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Podszywając się pod klienta wykonywali transakcje polegające na przelaniu pieniędzy na swoje konta[378].

Sprawca *spoofingu* swoim zachowaniem wyczerpuje znamiona czynu z art. 267 § 1 k.k. (kradzież informacji)[379], zagrożonego karą grzywny, karą ograniczenia wolności albo karą pozbawienia wolności do lat 2.

3. Bezpieczeństwo w bankowości internetowej

Według J. Pelczarskiego, dyrektora Departamentu Informatyki Pierwszego Polsko-Amerykańskiego Banku w Krakowie, technologia dokonywania operacji bankowych za pośrednictwem Internetu jest wystarczająco dojrzała i bezpieczna. Poziom bezpieczeństwa jest porównywalny, jak przy korzystaniu z teleserwisu, kart kredytowych czy rozwiązań typu *home/corporate banking*. Jednakże banki powinny podchodzić do bezpieczeństwa usług internetowych z największą ostrożnością, gdyż Internet jest siecią otwartą, podatną na ingerencję z zewnątrz i wymaga stosowania wielu zabezpieczeń. Dlatego też nieustannie prowadzone są prace nad rozwojem sposobów zabezpieczania danych. Rodzaje zabezpieczeń muszą ulegać nieustannej ewolucji, gdyż jak powszechnie wiadomo, nie ma absolutnie bezpiecznego systemu, który by w pełni zabezpieczał bankowe operacje elektroniczne[380].

Bez wątpienia podstawą funkcjonowania bankowości internetowej jest niezaprzeczalność transakcji autoryzowanej kodem, który jest znany wyłącznie posiadaczowi rachunku bankowego[381]. Zatem najistotniejszą cechą transakcji dokonywanych w bankowości internetowej jest ich autoryzacja, która polega na wprowadzeniu do systemu bankowości internetowej odpowiednich kodów autoryzacyjnych. Jeżeli zatem rozważamy kwestie związane z bezpieczeństwem w bankowości internetowej, to należy zaznaczyć, iż głównym elementem tego typu transakcji jest poufność danych wykorzystywanych do autoryzacji dokonanych transakcji (haseł dostępu, loginów, numerów kart kredytowych itp.).

[378] Źródło: http://bankowoscinternetowa.republika.pl/html/Bezp.html (dostęp 22.01.2012).
[379] Zob. Siemkowicz P.: op. cit., s. 7.
[380] Świecka B.: op. cit., s. 102.
[381] Szwajkowska G. i in.: op. cit., s. 29.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Zdaniem Szwajkowskiej i innych autorów, głównymi sposobami na zapewnienia bezpieczeństwa transakcji dokonywanych w Internecie są:

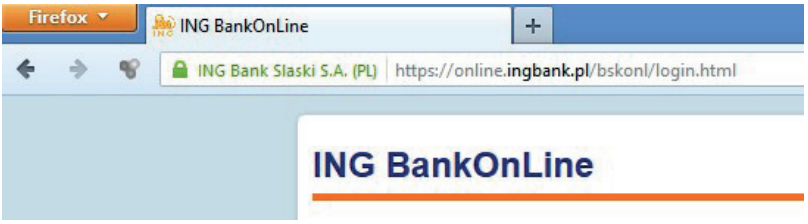
1) szyfrowana transmisja danych – realizowana z wykorzystaniem protokołu SSL,
2) proste uwierzytelnianie – identyfikator, hasło, kod PIN,
3) silne uwierzytelnianie – token, certyfikat użytkownika, klucz prywatny,
4) kwalifikowany podpis elektroniczny[382].

Protokół SSL (Secure Socket Layer), służy do bezpiecznej transmisji zaszyfrowanego strumienia danych i jest podstawą funkcjonujących obecnie systemów bankowości internetowej. Główne funkcje protokołu SSL, to:

- uwierzytelnianie – możliwość zweryfikowania tożsamości klienta i banku,
- poufność – możliwość szyfrowania przesyłanych informacji, które są czytelne wyłącznie dla komunikujących się stron,
- integralność – zabezpieczenie przed zmianą zawartości przesyłanego komunikatu[383].

Protokół SSL jest w chwili obecnej wykorzystywany i obsługiwany przez wszystkie przeglądarki internetowe. Nawiązanie bezpiecznego połączenia jest sygnalizowane osobie korzystającej z przeglądarki internetowej i, w zależności od jej rodzaju, może różnie być różnie obrazowane. Najczęściej jest to symbol zamkniętej kłódki i dodanie litery „s" przy adresie internetowym. Przykłady obrazują zamieszczone poniżej ryciny.

Rysunek 45. Przykład bezpiecznego logowania się na stronie internetowej w przeglądarce Mozilla Firefox na stronie banku ING Bank Śląski SA

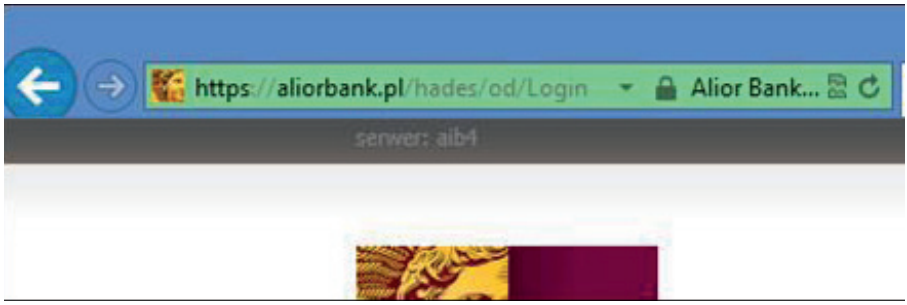


Źródło: Opracowanie własne.

[382] Ibidem.
[383] Ibidem, s. 30.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

Rysunek 46. Przykład bezpiecznego logowania się na stronie internetowej w przeglądarce Internet Explorer na stronie AliorBanku



Źródło: Opracowanie własne.

Jeżeli chodzi o proces uwierzytelniania, to należy pamiętać, iż każdemu klientowi korzystającemu z bankowości internetowej, bank nadaje indywidualny identyfikator użytkownika. W połączeniu ze wspomnianym identyfikatorem i w zależności od systemu bankowości internetowej oraz rodzaju wykonywanej operacji, można wyróżnić następujące metody uwierzytelniania[384]:

- stałe hasło,
- hasło jednorazowe (lista haseł jednorazowych, karta TAN *(Transaction Authorisation Number)*, token sprzętowy, token w postaci aplikacji w telefonie komórkowym, wiadomość SMS,
- certyfikaty cyfrowe, które skojarzone są z numerem PIN lub hasłem.

Jak zaznacza Szwajkowska i inni autorzy, systemy bankowości internetowej stosowane obecnie przez banki działające w Polsce wymagają autoryzacji transakcji, która przebiega co najmniej w dwóch etapach:

1. Uzyskanie dostępu do możliwości przeglądania rachunków – wymaga jedynie podania identyfikatora użytkownika i całego lub części (losowo wybranych znaków) hasła.
2. Wykonanie jakiejkolwiek transakcji – wymaga dokonania dodatkowej autoryzacji, która może być dokonana najczęściej w postaci podania kodu jednorazowego[385].

Bez wątpienia najważniejszą zasadą postępowania klienta baku powinna stać się ochrona poufności danych służących do autoryzacji usług

[384] Ibidem.
[385] Ibidem, s. 31.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

bankowości internetowej. Dane te są łakomym kąskiem dla przestępców, co wykazane zostało w przedmiotowym rozdziale.

Ataków, mających na celu pozyskanie danych autoryzacyjnych, z roku na rok jest coraz więcej, ale coraz lepsze stają się również zabezpieczenia strzegące przed tego typu atakami, zwłaszcza w bankach. Zdaniem Kaszubskiego, dyrektora Rady Bankowości Elektronicznej ZBP, Polska jest na najwyższym światowym poziomie w dziedzinie zabezpieczeń bankowych. Biorąc pod uwagę wszystkie ataki, które były do tej pory wymierzone w polskie banki, nie było ani jednego udanego ataku na bank. Zdarzały się natomiast ataki na klientów[386]. P. Jaroszewski , specjalista ds. Bezpieczeństwa Sieciowego NASK CERT Polska, stwierdza, że ponieważ technologie zabezpieczeń na przestrzeni ostatnich 15 lat są coraz lepsze, więc głównym czynnikiem ataku stał się człowiek, jako najsłabsze ogniwo systemu zabezpieczeń w bankowości elektronicznej[387].

Mając na uwadze bezpieczeństwo bankowości internetowej, ZBP opracował praktyczny poradnik zawierający podstawowe informacje i zasady, o których warto pamiętać podczas korzystania z usług bankowych świadczonych drogą elektroniczną[388]. Oto one:

Zasady ogólne:

1. **Pamiętaj, żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.**

   Banki nigdy nie podają w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie przekazując swoje poufne dane. Bezzwłocznie skontaktuj się ze swoim Bankiem i poinformuj o zdarzeniu.

2. **Sprawdź na stronie twojego banku jakie zabezpieczenia stosowane są w serwisie internetowym.**

   Przy każdym logowaniu bezwzględnie stosuj się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast skontaktuj się z pracownikiem Banku.

[386] „Hak w sieci" Fakty TVN – emisja w dniu 27.01.2012 r. godz. 19:00.
[387] Ibidem.
[388] Źródło: http://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa (dostęp 10.03.2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

3. **Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany.**

   Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy *firewall*. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.

4. **Dokonuj płatności internetowych tylko z wykorzystaniem pewnych komputerów.**

   Nie dokonuj płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.

5. **Skontaktuj się ze swoim dostawcą Internetu w celu upewnienia się, że korzysta on bezpiecznych kanałów dystrybucji tej usługi.**

   Zwracaj szczególną uwagę na jakość i bezpieczeństwo usług internetowych dostarczanych przez twojego dostawcę. Jeśli masz jakieś wątpliwości w tym zakresie zawsze masz prawo zapytać się dostawcy o jakość bezpieczeństwa oferowanego przez niego.

6. **Instaluj na swoim komputerze tylko legalne oprogramowanie.**

   Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.

7. **Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.**

   Większość programów antywirusowych przy włączonym monitorze antywirusowym ma detekcję (wykrywalność) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, których detekcja monitora antywirusowego jest niższa aniżeli skanera, powoduje to jednak lukę w systemie bezpieczeństwa.

8. **Aktualizuj system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe.**

   Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty", których celem jest

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk.

9. **Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia.**

   Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań.

10. **Unikaj stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje.**

    Szczególnie niebezpieczne mogą być strony internetowe zawierające treści pornograficzne. Ponadto z pozoru niewinne strony zawierające programy typu *freeware* również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często dekompilują je uzupełniając o złośliwy kod.

Zasady dotyczące płatności z internetowego konta bankowego:

11. **Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.**
12. **Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast zgłoś problem do swojego banku.**
13. **Nie wchodź na stronę internetową Twojego banku za pośrednictwem linków znajdujących się w przychodzących do ciebie mailach (*phishing*).**

    Używaj do tego celu adresu podanego ci przez Bank, z którym podpisał(aś/eś) umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „zakładek" (Firefox) lub „adresów ulubionych" (Internet Explorer), gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.

14. **Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony logowania twojego banku.**

    Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.

15. **Przed zalogowaniem sprawdź, czy połączenie z bankiem jest bezpieczne.**

    Adres witryny internetowej twojego banku powinien rozpoczynać się od skrótu: „https://", a nie „http://". Brak litery „s" w skrócie „http" oznacza brak szyfrowania, czyli, że twoje dane są transmitowane przez Internet tekstem jawnym, co naraża cię na ogromne niebezpieczeństwo.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

16. **Sprawdzaj prawidłowość certyfikatu.**

    Zanim wpiszesz identyfikator bądź login i hasło sprawdź, czy połączenie z bankiem odbywa się z wykorzystaniem szyfrowania. Jeżeli znajdziesz symbol kłódki, kliknij na niego dwa razy, aby sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla twojego banku. Jeśli certyfikat utracił ważność lub nie został wystawiony dla twojego banku albo nie można go zweryfikować zrezygnuj z połączenia.

17. **Nigdy nie udostępniaj osobom trzecim identyfikatora ani hasła dostępu.**

    Identyfikator jest poufnym numerem nadawanym przez bank, nie możesz go zmienić.

18. **Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie.**

    Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego na tobie nie wymusi zmieniaj je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr.

19. **Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.**

20. **Korzystaj z infolinii udostępnionej przez twój bank.**

    Zawsze masz prawo skorzystać z infolinii swojego banku jeśli masz wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem Internetu.

21. **Odwiedzaj regularnie portal „Bezpieczny Bank" na stronie internetowej ZBP – www.zbp.pl**

    Jeśli chcesz wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową regularnie odwiedzaj ten portal. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.

Zasady dotyczące płatności kartami płatniczymi przez Internet:

22. **Zachowaj rozwagę przy przekazywaniu numeru karty.**

    Nie należy udostępniać numeru karty nikomu, kto do nas dzwoni, również w sytuacji, gdy osoba dzwoniąca informuje, że są problemy z komputerem i proszą o weryfikację informacji. Nie ma zwyczaju by firmy dzwoniły prosząc przez telefon o numer karty płatniczej. Jeżeli to my inicjujemy połączenie, również nie należy udostępniać numeru

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

karty przez telefon, gdy nie mamy pewności, że rozmówca zasługuje na zaufanie.

23. **Nigdy nie odpowiadaj na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie – zgłoś taką sytuację w swoim banku.**

    Nigdy też nie odpowiadaj na maile, które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywany *phishingiem.*

24. **Nigdy nie podawaj informacji o karcie na stronach, które nie są bezpieczne.**

    Przykładowo strony z treściami pornograficznymi lub strony nieznanych szerzej firm oferujące markowy towar po rewelacyjnych cenach. Przed wprowadzeniu numeru karty w formularzu na stronie należy upewnić się, czy dane przesyłane z formularza są odpowiednio chronione (czyli – upraszczając – czy adres strony z formularzem rozpoczyna się od https i czy strona posiada odpowiednie certyfikaty – te informacje podaje przeglądarka, zazwyczaj w pasku statusu na dole okna).

25. **Nie zapisuj kodu PIN na karcie, ani nie przechowuj go razem z kartą.**

    W takich okolicznościach nie tylko działasz niezgodnie z przepisami prawa, ale także w przypadku kradzieży portfela czy portmonetki i posłużenia się twoją kartą płatniczą bank będzie zwolniony z obowiązku pokrycia powstałej szkody.

26. **Chroń swój numer karty i inne poufne kody umożliwiające dokonane transakcji np. numer PIN, numer CVV2 lub CVC2 – ostatnie trzy cyfry numeru umieszczonego na pasku do podpisu na odwrocie karty.**

    Przestępcy mogą wchodzić w ich posiadanie, rejestrując obraz karty np. przy użyciu telefonu komórkowego z aparatem fotograficznych, kamerą video lub w inny sposób.

27. **Dokonuj transakcji w znanych i zweryfikowanych przez siebie sklepach internetowych. W przypadku mniejszych serwisów zbadaj ich wiarygodność, na przykład dzwoniąc do takiego serwisu i weryfikując jego ofertę, warunki dokonania transakcji oraz reklamacji.**

    Upewnij się, czy nie jesteś na stronie internetowej podszywającej się pod stronę twojego banku/sklepu (podobna nazwa i wygląd strony, którą posługują się nieuczciwi naśladowcy w celu zmylenia i wyłudzenia

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353

pieniędzy). Zapoznaj się z regulaminem sklepu internetowego, a szczególnie z informacjami dotyczącymi bezpieczeństwa transakcji. Przed dokonaniem transakcji upewnij się, że transmisja odbywa się w bezpiecznym połączeniu za pomocą protokołu SSL/TLS.

Warto w tym miejscu powiedzieć kilka słów na temat tego, jak zdaniem ZBP, banki dbają o bezpieczeństwo swoich klientów. Podstawowe formy ochrony, to[389]:

- Podstawowa identyfikacja klienta: – identyfikator + PIN, tonek, token + PIN.
- Protokół szyfrowania transmisji danych w Internecie – SSL.
- Dostęp w oparciu o certyfikaty.
- Kody wysyłane SMS'em.
- Jednorazowe kody autoryzujące transakcje.
- Podpis elektroniczny, funkcja skrótu i jej zastosowanie.
- Karty mikroprocesorowe z zapisanym certyfikatem.
- Limity transakcji.
- Automatyczne wygasanie sesji po okresie nieaktywności użytkownika.

Reasumując, podkreślić należy, iż klient banku powinien należycie dbać o dane wrażliwe, którymi w przypadku bankowości elektronicznej są: wszelkie dane osobowe, hasła, numery kart płatniczych i elektroniczne dokumenty zawierające dane bankowe. Są one bowiem łakomym kąskiem dla wszelkiego rodzaju przestępców.

[389] Ibidem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 15535453A6439353